

Appeal No. 2024-2256

**IN THE UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT**

LARRY GOLDEN,

Plaintiff-Appellant,

v.

UNITED STATES,

Defendant-Appellee

On Appeal from the United States Court of Federal Claims in
Case No. 1:23-cv-00811, Senior Judge Eric G. Bruggink

**SUPPLEMENTAL APPENDIX
PURSUANT TO FED. CIR. R. 30(e)**

BRIAN M. BOYNTON
*Principal Deputy
Assistant Attorney General*

SCOTT BOLDEN
Director

GRANT D. JOHNSON
Trial Attorney
Commercial Litigation Branch
Civil Division
Department of Justice
Washington, DC 20530
(202) 305-2513

Of Counsel:
CONRAD J. DeWITTE, JR.
Department of Justice

TABLE OF CONTENTS

Pages**

Appealed-From Orders

April 23, 2024 Order Dismissing Plaintiff's Case
Pursuant to RCFC 12(b)(6) (Dkt. 28) .. SAppx1001–1007

July 30, 2024 Order Denying Plaintiff's Motion
for Reconsideration (Dkt. 31) SAppx1008–1012

Patents-In-Suit

U.S. Patent No. 9,096,189 SAppx1013–1039

U.S. Patent No. 9,589,439 SAppx1040–1069

U.S. Patent No. 10,163,287 SAppx1070–1096

Larry Golden v. United States (CFC Case No. 23-811)

Docket Sheet SAppx1097–1099

Complaint (Dkt. 1) SAppx1100–1133

Plaintiff's August 22, 2021 Corrected Preliminary
Infringement Contentions in *Golden v.*
United States (CFC Case No. 13-307)
(Exhibit 2 to the Government's Motion
to Dismiss) (Dkt. 10-2)..... SAppx1134–1142

****Note**—The Supplemental Appendix begins at SAppx1001 to ensure it does not overlap in pagination with any Appendix provided by Plaintiff-Appellant. See Electronic Filing Procedures, Federal Circuit (Ver. 3.2.2) at 35.

CORRECTED

In the United States Court of Federal Claims

No. 23-811C
(Filed: April 23, 2024)

LARRY GOLDEN,

Plaintiff,

v.

THE UNITED STATES,

Defendant.

Larry Golden, pro se.

Grant Johnson, Trial Attorney, United States Department of Justice, Civil Division, Commercial Litigation Branch, Washington, DC, with whom were *Brian M. Boynton*, Principal Deputy Assistant Attorney General, and *Scott Bolden*, Director, for defendant.

ORDER

BRUGGINK, *Judge*

Plaintiff Larry Golden, appearing *pro se*, filed his most recent, fourth complaint in this court on May 31, 2023. In it, Mr. Golden alleges the United States, through the Defense Threat Reduction Agency “authorized or consented” to the use of Google phones that infringed on the same patents¹ as those previously asserted in his first case, filed in 2013 (“*Golden I*”). Compl. ¶ 21 (the present case is “*Golden IV*”). Except for the manufacturer of the accused devices and the agency alleged to have authorized the

¹ Those are U.S. Patents No. 10,163,287, 9,589,439, and 9,096,189. A fourth patent, not asserted in this case, was also alleged to have been infringed in *Golden I*.

infringing use, the present case is otherwise virtually identical to plaintiff's first patent complaint.

In *Golden I* (Case No. 13-307), plaintiff alleged that the government infringed the claims of five related patents through a Department of Homeland Security ("DHS") initiative known as "CELL-ALL." Eventually, he identified virtually all cell phones manufactured by Apple and Samsung after the 2011 DHS initiative as infringing. After plaintiff amended his complaint six times, *Golden I* was dismissed on November 10, 2021, with prejudice for failure to conform his infringement contentions to the court's rules. *Golden v. United States*, 156 Fed. Cl. 623, 632 (2021). Plaintiff appealed, and the Federal Circuit affirmed the dismissal on September 8, 2022. *Golden v. United States*, No. 2022-1196, 2022 WL 4103287 (Fed. Cir. 2022). Mr. Golden also filed two other actions in this court, founded on constitutional theories, which are not germane to the present issues.²

Mr. Golden also recently brought his theories to the federal district courts in South Carolina and California, asserting similar patent claims to those here against Google and other companies. We need not discuss all of the litigation that those complaints have spawned. What is relevant here, however, is that Mr. Golden filed infringement claims against Apple, and others, in the District of South Carolina which were dismissed as frivolous. On appeal, however, the Federal Circuit reversed, holding that the Apple

² Plaintiff filed his second action on January 17, 2019, alleging a Fifth Amendment taking based on the Patent Trial & Appeal Board's cancellation of certain claims of another of plaintiff's patents during an *inter partes* review ("IPR") ("*Golden II*"). The court dismissed *Golden II* with prejudice on May 14, 2019, finding that the cancellation of the patent claims was plainly the result of plaintiff's voluntary amendment, not government action. *Golden v. United States*, No. 19-104C, 2019 WL 2056662 (Fed. Cl. 2019) ("*Golden II*"). The Federal Circuit also affirmed this dismissal. *Golden v. United States*, 955 F.3d 981 (Fed. Cir. 2020).

Plaintiff filed his third action here on February 7, 2023, again on the grounds that DHS took one of his patents during the IPR without compensating him. *See Golden v. United States*, No. 23-185C, 2023 WL 4466401 (Fed. Cl. May 30, 2023) ("*Golden III*"). Before granting the government's motion to dismiss for lack of jurisdiction on statute of limitations grounds, we noted that *res judicata* would otherwise clearly bar the claim due to its near-identical nature to the claims proposed in *Golden II*. *Id.*, *aff'd*, No. 2023-2139, 2023 WL 8663093 (Fed. Cir. Dec. 15, 2023).

complaint was not facially frivolous, but the court took no position on the merits of the infringement claim itself. *Golden v. Apple, Inc.*, No. 2022-1229, 2022 WL 4103285 (Fed. Cir. Sept. 8, 2022). As discussed later, a misunderstanding of the import of that decision was the impetus for plaintiff’s instant case.

In the present suit, defendant has moved to dismiss on the basis that Mr. Golden’s claim is barred due to the preclusive effect of the judgment entered in *Golden I*.³ Plaintiff has since filed a motion for summary judgment, arguing that the Federal Circuit’s reversal of the South Carolina district’s dismissal is grounds for judgment in his favor here. Mr. Golden notes in that motion that the elements of the accused devices in this case and those in the South Carolina case are “virtually identical.” Mr. Golden also filed a motion for disqualification of the undersigned on the grounds of coercion and “difficulty,” or, in the alternative, bias. Lastly, plaintiff filed two motions for judicial notice, the first regarding certain facts he believes relevant to his theory of infringement, and the second concerning filings he made in one of his cases in the Northern District of California.⁴ Because, as explained below, the complaint fails to state a claim upon which relief can be granted, we need not reach any of the latter motions. The motion for disqualification we deny.

Defendant argues that plaintiff’s claims against the government accusing Google phones are barred by the doctrine of claim preclusion, traditionally known as *res judicata*, because the newly accused devices are virtually identical to the devices he has previously accused. The government argues that, because his prior case was dismissed with prejudice, which operates as a judgment of non-infringement, his new claim is also barred because it has already been decided. *See Hallco Mfg. Co. v. Foster*, 256 F.3d 1290, 1297 (Fed. Cir. 2001) (“a dismissal with prejudice . . . is a judgment on the merits”). Put another way, because there is no practical difference, at least as to the features alleged to be infringing, between the Google phones now accused and the Apple and Samsung products previously accused, there is nothing new to be decided now. The thing has been decided

³ Defendant also argues that plaintiff’s theory of infringement is facially defective and fails to state a claim. We do not reach this issue because the complaint is plainly barred by *res judicata* and the associated *Kessler* doctrine.

⁴ Plaintiff also filed a motion to strike defendant’s motion to dismiss, which we denied by order on July 31, 2023.

(“*res judicata*”). Further, to the extent that our judgment in *Golden I* would not cover any alleged infringement post-dating that judgment, defendant argues that the *Kessler* doctrine expands the reach of claim preclusion to cover those allegations as well. *Kessler v. Eldred*, 206 U.S. 285 (1907) (206 U.S. 285 (1907) (Holding that a judgment of a product’s non-infringement may not be re-litigated, even if the parties are different and the alleged infringement post-dates the earlier judgment)).

The doctrine of *res judicata* prevents re-litigation of claims previously decided. See generally *Sharp Kabushiki Kaisha v. ThinkSharp, Inc.*, 448 F.3d 1368, 1372 (Fed. Cir. 2006). The current complaint, however, is aimed at different infringing devices, Google phones, not expressly implicated in *Golden I*. Defendant, however, argues that, because there is no substantive difference between the phones now implicated by the present complaint and those alleged to be infringing in the earlier case, claim preclusion applies. We agree.

In the Federal Circuit, claim preclusion in a patent suit generally applies “when a patentee seeks to assert the same patent against the same party and the same subject matter.” *Senju Pharm. Co. v. Apotex Inc.*, 746 F.3d 1344, 1349 (Fed. Cir. 2014). The same patents and the same parties are clearly involved. The question then is whether the Google phones are the same as the subject of the previous suit. They are, of course, not literally the same phones. As defendant rightly points out, however, the subject matter is the same for claim preclusion in an infringement suit if the formerly accused and the newly accused devices are “essentially the same.” *Foster v. Hallco Mfg. Co., Inc.*, 947 F.2d 469, 479-80 (Fed. Cir. 1992). They are essentially the same if the new devices are “materially identical . . . [to the earlier devices] with respect to the pertinent claim limitations at issue.” *Nystrom v. Trex co., Inc.*, 580 F.3d 1281, 1286 (Fed. Cir. 2009). The focus is thus on what is claimed to be infringing in the new devices to see whether it is “essentially the same” as what was claimed to have been infringing in the old devices. Here, as explained below, the elements in these new phones that Mr. Golden alleges to be infringing are the same as those he claimed to be infringing in *Golden I*. Thus, claim preclusion applies, at least as to pre-*Golden I* judgment infringement.⁵

⁵ Any alleged infringing acts after the judgment in *Golden I* are not barred by claim preclusion because they do not arise from the same transactional facts, or “infringing acts.” Definitionally, post-judgment infringement cannot be the same acts already considered, and thus the claims cannot be the same for purposes of claim preclusion. See, e.g., *Brain Life, LLC v. Elektra Inc.*, 746 F.3d 1045, 1054 (Fed. Cir. 2014). Absent the *Kessler*

In the present complaint, Mr. Golden concedes that his current claim is “virtually identical” in that “the results are the same” when compared to devices also accused in *Golden I*. Compl. ¶ 17; *see also* ¶¶ 18-20. Further illustrating that the subject matter is essentially the same in this suit as his first, the complaint also contains a comparison between the Google Pixel 5 phone and the Apple iPhone 12, Samsung Galaxy S21, and LG V60 phones. The latter three of those phones were all accused by plaintiff in *Golden I*, as evidenced by the Corrected Claim Chart filed by Mr. Golden there, excerpts of which were appended to defendant’s motion to dismiss in this docket, which we treat as judicial admissions by Mr. Golden. Plaintiff went on to explain on page 13 of the present complaint that the use of the Pixel 5 phone is illustrative of the infringement of the other Google phones that he is accusing in this suit. Thus we are assured that all of the newly alleged infringement overlaps with what he claimed in *Golden I*. Even a cursory review of the rest of the present complaint—the comparison of devices mentioned above—reveals that they are materially identical to the charts filed in *Golden I*. The same elements of the Apple, Samsung, and LG phones alleged to be infringing in the first suit are what he accuses now in the Google phones, as illustrated by the Pixel 5 claim chart in his complaint (e.g., a central processing unit, GPS, wifi or Bluetooth connectivity, and biometrics). In fact, he performs the comparison himself in the present complaint again by including a comparison of the Apple, Samsung and LG devices with the Google Pixel 5. The subject of the two suits is “essentially the same” because the devices are identical with respect to the elements plaintiff claims are infringing.

The Federal Circuit has on several instances stated that claim preclusion has a temporal limitation as to the date of the preclusive judgment. *E.g., In re PersonalWeb Techs. LLC*, 961 F.3d 1365, 1376 (Fed. Cir. 2020). The government thus invokes the *Kessler* doctrine as covering the “temporal limitation” gap of claim preclusion. In *Kessler v. Eldred*, the Supreme Court adopted an enlargement of traditional claim and issue preclusion doctrines to further preserve the utility of previous judgments of non-infringement by holding that a prior judgment of non-infringement would bar new

doctrine, the issue of whether a prior judgment of non-infringement was preclusive of post-judgment acts would be considered under the rubric of issue preclusion, also known as collateral estoppel. Collateral estoppel was not raised by the government, nor need it have been, because, in the patent context, as will be discussed below, *Kessler* enlarges the reach of non-infringement judgments, or, as defendant puts it, bridges the temporal gap left by claim preclusion.

infringement claims for post-judgment acts, against third parties, and covering very similar accused devices. 206 U.S. 285 (1907); *see also SpeedTrack, Inc. v. Office Depot, Inc.*, 971 F.3d 1317, 1318 (Fed. Cir. 2015) (recognizing that, absent *Kessler*, patent holders could escape prior judgments of non-infringement by suing customers of the earlier defendant for post-judgment infringement). The key issue is whether the accused devices are the same or “essentially the same,” just as with claim preclusion. *Brain Life, LLC v. Elektra Inc.*, 746 F.3d 1045, 1057 (Fed. Cir. 2014). If so, pursuant to *Kessler*, a trade right in the devices attaches after a judgment of non-infringement and those devices, along with others that are “essentially the same,” are protected from future allegations of infringement. *In re PersonalWeb*, 961 F.3d at 1379. As explained above, the newly accused devices are essentially the same as those previously accused, and thus doctrines of *res judicata* and *Kessler* preclude litigating these issues against the government again.

Plaintiff’s only argument is that, because the Federal Circuit reversed and remanded the decision of the District Court for South Carolina in *Golden v. Apple Inc.*, we should overlook *Kessler*. In Mr. Golden’s view of the circuit’s opinion, infringement has been established. That, however, is a dramatic misreading of the appellate opinion. The Federal Circuit was careful to note that it “express[ed] no opinion as to the adequacy of the complaint or claim chart except that it is not facially frivolous.” *Golden v. Apple Inc.*, No. 2022-1229, 2022 WL 4103285, at *2 (Fed. Cir. Sept. 8, 2022). Nothing in the Federal Circuit’s opinion is germane to the questions of claim preclusion and the *Kessler* doctrine, both of which we find preclude consideration of the present complaint because the devices accused are, as conceded by plaintiff, “virtually identical,” or “essentially the same” as those already adjudged in the first suit, *Golden I. Compl.* ¶17.

The Federal Circuit was recently confronted with a similar situation in which the patentee had infringement claims dismissed with prejudice for discovery abuses. When that patentee brought a later suit, accusing different devices, the district court dismissed it, *inter alia*, as precluded by *Kessler*. The Federal Circuit affirmed, holding that a dismissal with prejudice, whatever the underlying reason, is a judgment of non-infringement for purposes of the *Kessler* doctrine. *Askan v. FARO Techs., Inc.*, 2023 WL 4101351, at *3 (Fed. Cir. June 21, 2023). Thus, because the devices were found to be essentially the same, *Kessler* applied. *Id.* at *4. Here, Mr. Golden’s claims in his first suit were dismissed with prejudice. 156 Fed. Cl. at 632. As explained above, the newly accused devices are essentially the same as those previously alleged to be infringing, as plaintiff admits. Thus,

Kessler applies, and the present claim is barred. Accordingly, the following is ordered:

1. Plaintiff's motion seeking disqualification of the undersigned is denied.
2. Defendant's motion to dismiss is granted.
3. The Clerk of Court is directed to dismiss the complaint pursuant to rule 12(b)(6) for failure to state a claim.
4. All other motions are denied as moot.

s/ Eric G. Bruggink
ERIC G. BRUGGINK
Senior Judge

In the United States Court of Federal Claims

No. 23-811C

(Filed: July 30, 2024)

* * * * *

LARRY GOLDEN,

Plaintiff,

v.

THE UNITED STATES,

Defendant.

* * * * *

ORDER ON RECONSIDERATION

Plaintiff Larry Golden, appearing *pro se*, filed his fourth complaint in this court on May 31, 2023, alleging that the United States government, acting through the Defense Threat Reduction Agency (“DTRA”), implicitly authorized the use of three of his patents by several third party corporations in violation of 28 U.S.C. § 1498(a). On April 23, 2024, the court dismissed plaintiff’s claim pursuant to Rule 12(b)(6) of the Rules of the United States Court of Federal Claims (“RCFC”), finding that his claim was barred by claim preclusion and the related *Kessler* doctrine. *Golden v. United States*, 171 Fed. Cl. 33, 37 (2024) (relying on *Kessler v. Eldred*, 206 U.S. 285 (1907)). Plaintiff filed a motion for reconsideration and notice of pending motion for disqualification on April 30, 2024, asserting that the court’s dismissal of his claim had been rooted in racial bias and was not in accordance with the doctrine of vertical *stare decisis*.

Turning to the present motion, although denominated as a motion for reconsideration, it appears that the thrust of the motion is aimed at disqualification of the undersigned, but we note that most of the arguments in support of that relief are disagreements with the merits of our dismissal decision.¹ We begin by noting that there is no provision in the court’s rules

¹ We are unsure if plaintiff’s notice of pending motion for disqualification is a reference to his earlier-filed motion, which was disposed of in our opinion

for the filing of a post-judgment motion for disqualification. Plaintiff cites 28 U.S.C. § 144 as grounds for the requested disqualification. That statute, by its very terms, however, applies only to the federal district courts, and not to the Court of Federal Claims. 28 U.S.C. § 144 (“Whenever a party . . . *in a district court* makes and files a timely and sufficient affidavit that the judge before whom the matter is pending has a personal bias or prejudice . . . such judge shall proceed no further therein.”) (emphasis added). Nor would such a request be timely after judgment has been entered. We thus consider the motion under the rubric of reconsideration.

Motions for reconsideration are governed by Rule 59(a)(1) of the Rules of the United States Court of Federal Claims (“RCFC”). Pursuant to Rule 59(a)(1)(A), “the court may, on motion, grant . . . a motion for reconsideration on all or some of the issues . . . for any reason for which a new trial has heretofore been granted in an action at law in federal court.” A motion for reconsideration may also be granted “for any reason for which a rehearing has heretofore been granted in a suit in equity in federal court; or upon the showing of evidence . . . that any fraud, wrong, or injustice has been done to the United States.” RCFC 59(a)(1)(B–C). Specifically, RCFC 59 permits reconsideration for one of three reasons: 1) an intervening change in the controlling law has occurred; 2) previously unavailable evidence is now available; or 3) the motion is necessary to prevent manifest injustice. *Matthews v. United States*, 73 Fed. Cl. 524, 525 (2006). Furthermore, “the movant must point to a manifest error of law or mistake of fact” and must do more than “merely reassert[] arguments which were previously made and were carefully considered by the court.” *Henderson Cnty. Drainage Dist. No. 3 v. United States*, 55 Fed. Cl. 334, 337 (2003). A motion under RCFC 59 “must be based upon manifest error of law, or mistake of fact, and is not intended to give an unhappy litigant an additional chance to sway the court.” *Parsons ex rel. Linmar Prop. Mgmt. Tr. v. United States*, 174 Fed. Appx. 561, 563 (Fed. Cir. 2006).

Plaintiff does not argue a change in the controlling law or offer any newly discovered evidence. Instead his motion largely restates arguments he made in his complaint. Mr. Golden presents four broad reasons for why he believes our previous opinion should be reconsidered. First, he alleges that our opinion runs afoul of the doctrine of *stare decisis*. Second, he argues that his Fifth Amendment due process rights have been violated. Third, plaintiff argues that we misapplied the doctrine of res judicata, or claim preclusion. Fourth, plaintiff suggests throughout his motion that our opinion was

of April 23, or whether plaintiff intends to convey that he is asking for that same relief in this motion.

motivated by racial bias, though he does not point to any specific evidence or details that support this allegation. We address these four arguments in turn.

Plaintiff argues that the doctrine of *stare decisis* requires the Court of Federal Claims to follow the decisions of the Court of Appeals for the Federal Circuit, specifically the circuit court's decision in Mr. Golden's appeal from the dismissal of his claims in district court in South Carolina. We note, to start, that that decision is not the law of this case because it was not an appeal in this case. It is also unpublished and thus, by the circuit's own rules, not binding precedent. *See* Fed. Cir. R. 32.1(d). It is persuasive authority only to the extent that it prescribes some rule of law applicable to the issues in this case. It did not. The issue there was whether plaintiff's pleadings were facially frivolous. *Golden v. Apple Inc.*, No. 2022-1229, 2022 WL 4103285 (Fed. Cir. Sept. 8, 2022). The issue here was whether the doctrine of claim preclusion, as expanded by *Kessler*, barred relitigation of the issue of infringement. *Golden*, 171 Fed. Cl. at 37.

As we observed in our dismissal opinion, plaintiff has fundamentally misunderstood the Federal Circuit's ruling in *Golden v. Apple Inc.* The present motion raises no new argument in this regard, and the argument he does make hinges on a "dramatic misreading of the appellate opinion." *Id.*

Next, plaintiff alleges that his Fifth Amendment due process rights have been violated, because the court has allegedly deprived plaintiff of his property through "unfair and unjustified" means. Mot. Recons. 2. Though not clear, his argument seems to be that he should have won his case on its merits, and because he did not, his due process rights have been violated. Plaintiff has not identified any process that was due him and which was denied. His claims were barred by *res judicata*. That is not a violation of due process. *See Searcy v. Dep't of Agriculture*, 813 Fed. App'x 472, (Fed. Cir. 2011) (holding that the Merit Systems Protection Board did not violate the appellant's due process rights by *sua sponte* dismissing the claim as barred by *res judicata*). As the Supreme Court has explained, the fundamental requirements of procedural due process are notice and opportunity to respond, both of which are met here. *Cleveland Bd. Of Educ. v. Loudermill*, 470 U.S. 532, 546 (1985).

As to *res judicata* itself, plaintiff argues that "issue preclusion"² does not apply here and is inapplicable to his infringement claims. He calls the

² We understand plaintiff to actually be referring to claim preclusion, which was the grounds for his complaint's dismissal.

Kessler doctrine a “special” preclusion doctrine “created” by the Federal Circuit which should not apply here, because it supersedes congress’ intent to allow patent infringement suits to be brought against the government “whenever” under 28 U.S.C. § 1498(a). Mot. Recons. 4. Plaintiff is wrong. The doctrine of *res judicata* applies to all claims at law and equity. It protects the preclusive effect of judgments and preserves the court’s and prevailing parties’ resources by preventing relitigation of previously decided claims. *See Montana v. United States*, 440 U.S. 147, 153–154 (1979) (stating that *res judicata* protects against the “expense and vexation attending multiple lawsuits, conserves judicial resources,” and minimizes the “possibility of inconsistent decisions.”). We have applied *Kessler* before in the section 1498 context. *See, e.g., JG Techs., LLC v. United States*, 156 Fed. Cl. 691, 713 (2021) (finding that certain of plaintiff’s infringement claims against the United States were barred by *Kessler*).

In Mr. Golden’s view, we have unduly relied on the previous cases in which Golden lost. As explained in April, however, the doctrine, as expanded by *Kessler*, applies, and it bars plaintiff’s latest complaint. *Golden*, 171 Fed. Cl. at 37. This motion for reconsideration casts no doubt on that result.

Lastly, we address the allegations of racial bias which plaintiff peppers throughout his motion without substantiation or citation to evidence outside of his disagreement as to the disposition of his cases. An adverse result is not evidence, by itself, of bias. *See Liteky v. United States*, 510 U.S. 540, 555 (1994) (“[J]udicial rulings alone almost never constitute a valid basis for a bias or partiality motion.”). *See also Johnson v. Warden*, No. 2:16-cv-985, 2020 U.S. Dist. LEXIS 54236, at *49 (S.D. Ohio March 27, 2020) (“Evidence of racial bias cannot be inferred but must be clearly demonstrated in the record.”). In short, plaintiff has not presented any basis to reconsider on grounds of bias.

Plaintiff’s motion fails to demonstrate any bases for reconsideration under RCFC 59. Thus no response from defendant is necessary, and the motion is denied.³

³ Plaintiff also attempted to file a motion for status update regarding his motion for reconsideration. The clerk’s office received that document on July 17, 2024, but did not docket it because there is no provision in the court’s rules for the filing of such a motion. We allow the motion to be filed and deny it as moot.

s/Eric G. Bruggink
ERIC G. BRUGGINK
Senior Judge

(12) **United States Patent**
Golden

(10) **Patent No.:** **US 9,096,189 B2**
(45) **Date of Patent:** **Aug. 4, 2015**

(54) **MULTI SENSOR DETECTION, STALL TO STOP AND LOCK DISABLING SYSTEM**

USPC 340/539.1, 539.11, 539.13, 539.16, 340/539.17, 539.22, 539.25, 539.26, 540, 340/573.1, 574; 348/143; 380/228, 229, 380/232; 382/103, 115; 702/32
See application file for complete search history.

(71) Applicant: **Larry Golden**, Mauldin, SC (US)

(72) Inventor: **Larry Golden**, Mauldin, SC (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/021,693**

(22) Filed: **Sep. 9, 2013**

(65) **Prior Publication Data**

US 2014/0071274 A1 Mar. 13, 2014

Related U.S. Application Data

(60) Continuation of application No. 13/288,065, filed on Nov. 3, 2011, now Pat. No. 8,531,280, which is a division of application No. 12/802,001, filed on May 27, 2010, now Pat. No. 8,334,761, which is a continuation of application No. 12/657,356, filed on Jan. 20, 2010, now Pat. No. 8,106,752.

(51) **Int. Cl.**

B60R 25/10 (2013.01)
B60R 25/102 (2013.01)
B60R 25/01 (2013.01)
B60R 25/04 (2013.01)
G07C 9/00 (2006.01)
G08B 15/00 (2006.01)
G08B 21/12 (2006.01)

(52) **U.S. Cl.**

CPC **B60R 25/102** (2013.01); **B60R 25/018** (2013.01); **B60R 25/04** (2013.01); **G07C 9/00912** (2013.01); **G08B 15/00** (2013.01); **G08B 21/12** (2013.01); **B60R 2325/205** (2013.01); **B60R 2325/304** (2013.01); **G07C 2009/0092** (2013.01)

(58) **Field of Classification Search**

CPC ... B60R 2325/00; G08B 21/12; G08B 25/009

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,385,469 A 5/1983 Scheuerpflug
4,544,267 A 10/1985 Schiller
4,586,441 A 5/1986 Zekich
4,792,226 A 12/1988 Fishbine
5,222,152 A 6/1993 Fishbine

(Continued)

OTHER PUBLICATIONS

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 11/397,118; mailed Nov. 14, 2007; Alexandria, Virginia, USA; pp. 1-12; parent U.S. Appl. No. 13/288,065 (12 pages).

(Continued)

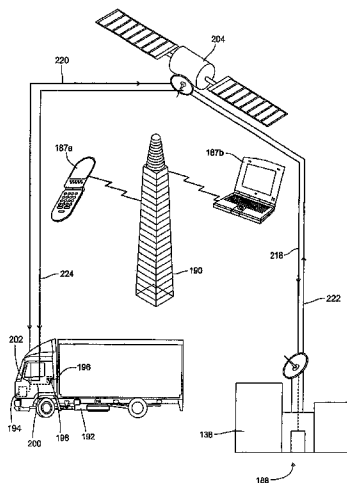
Primary Examiner — Van Trieu

(57)

ABSTRACT

A multi sensor detection and disabling lock system includes detector cases for holding interchangeable detectors that sample for chemical, biological and radiological compounds, agents and elements, with each detector case disposed in or upon the monitored product. The detector case transmits detection information to a monitoring computer terminal and transmits a signal to a lock disabler engaged to the product to lock or disable the product's lock thereby preventing untrained, unauthorized and unequipped individual's from gaining access and entry to the product, and also preventing further contamination of the area. The detection system can be interconnected to surveillance towers scanning detector cases disposed at seaport docks, freight depots and rail terminals for monitoring containers being prepared for shipment or sitting on docks for long periods of time.

9 Claims, 13 Drawing Sheets



US 9,096,189 B2

Page 2

(56)

References Cited

U.S. PATENT DOCUMENTS

5,223,844	A	6/1993	Mansell et al.	
5,233,404	A	8/1993	Lougheed	
5,557,254	A	9/1996	Johnson	
5,682,133	A	10/1997	Johnson	
5,766,956	A	6/1998	Groger	
5,938,706	A	8/1999	Feldman	
5,959,529	A	9/1999	Kail, IV	
5,963,657	A	10/1999	Bowker	
5,986,543	A	11/1999	Johnson	
5,990,785	A *	11/1999	Suda	340/426.21
6,049,269	A	4/2000	Byrd	
6,078,265	A	6/2000	Bonder	
6,262,656	B1	7/2001	Byrd	
6,271,745	B1	8/2001	Arizal	
6,374,652	B1	4/2002	Hwang	
6,411,887	B1	6/2002	Martens	
6,470,260	B2	10/2002	Martens	
6,542,076	B1	4/2003	Joao	
6,542,077	B2	4/2003	Joao	
6,588,635	B2	7/2003	Vor Keller	
6,610,977	B2	8/2003	Megerle	
6,613,571	B2	9/2003	Cordery	
6,628,813	B2	9/2003	Scott	
6,647,328	B2	11/2003	Walker	
6,738,697	B2	5/2004	Breed	
6,923,509	B1	8/2005	Barnett	
6,980,092	B2	12/2005	Turnbull	
6,988,026	B2	1/2006	Breed et al.	
7,005,982	B1	2/2006	Frank	
7,034,677	B2 *	4/2006	Steinthal et al.	340/539.12
7,034,683	B2	4/2006	Ghazarian	
7,103,460	B1	9/2006	Breed	
7,109,859	B2	9/2006	Peeters	
7,116,798	B1	10/2006	Chawla	
7,148,484	B2	12/2006	Craig et al.	
7,164,117	B2	1/2007	Breed et al.	
7,171,312	B2 *	1/2007	Steinthal et al.	702/32
7,243,945	B2	7/2007	Breed et al.	
7,339,469	B2	3/2008	Braun	
7,346,439	B2	3/2008	Bodin	
7,385,497	B2	6/2008	Golden	
7,397,363	B2	7/2008	Joao	
7,636,033	B2	12/2009	Golden	
7,647,180	B2	1/2010	Breed	
7,844,505	B1	11/2010	Arneson et al.	
7,868,912	B2 *	1/2011	Venetianer et al.	348/143
7,872,575	B2	1/2011	Tabé	
7,880,767	B2 *	2/2011	Chinigo	348/148
7,961,094	B2	6/2011	Breed	
8,274,377	B2	9/2012	Smith et al.	
8,531,521	B2 *	9/2013	Romanowich	348/143
8,564,661	B2 *	10/2013	Lipton et al.	348/143
2002/0145666	A1 *	10/2002	Scaman et al.	348/148
2003/0063004	A1 *	4/2003	Anthony et al.	340/574
2003/0137426	A1 *	7/2003	Anthony et al.	340/574
2003/0206102	A1	11/2003	Joao	
2004/0107028	A1	6/2004	Catalano	
2004/0222092	A1	11/2004	Musho	
2005/0195069	A1	9/2005	Dunand	
2006/0164239	A1	7/2006	Loda	
2006/0176169	A1 *	8/2006	Doolin et al.	340/521
2006/0181413	A1	8/2006	Mostov	
2006/0250235	A1	11/2006	Astrin	
2007/0171042	A1	7/2007	Metes et al.	
2008/0045156	A1	2/2008	Sakhpara	
2008/0122595	A1	5/2008	Yamamichi	
2008/0234907	A1	9/2008	Labuhn	
2010/0159983	A1	6/2010	Golden	
2011/0178655	A1	7/2011	Golden	

OTHER PUBLICATIONS

United States Patent and Trademark Office; Office Action from U.S. 12/155,573; mailed Apr. 9, 2009; Alexandria, Virginia, USA; pp. 1-7; parent U.S. Appl. No. 13/288,065 (7 pages).

United States Patent and Trademark Office; Office Action from U.S. 12/155,573; mailed Jul. 30, 2009; Alexandria, Virginia, USA; pp. 1-9; parent U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Notice of Allowability from U.S. 12/155,573; mailed Oct. 28, 2009; Alexandria, Virginia, USA; pp. 1-5; parent U.S. Appl. No. 13/288,065 (5 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/657,356; mailed Jul. 12, 2010; Alexandria, Virginia, USA; pp. 1-14; parent U.S. Appl. No. 13/288,065 (14 pages).

United States Patent and Trademark Office; Notice of Allowability from U.S. 12/657,356; mailed Mar. 10, 2011; Alexandria, Virginia, USA; pp. 1-4; parent U.S. Appl. No. 13/288,065 (4 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 13/065,837; mailed Jul. 18, 2011; Alexandria, Virginia, USA; pp. 1-9; parent U.S. Appl. No. 13/288,065 (4 pages).

A newspaper article of Mr. Melvin Sullivan and his family that references the date, Mar. 6, 2001; parent U.S. Appl. No. 13/288,065.

A letter of response Mr. Sullivan received from Pfeiffer & Gantt, PA, dated Sep. 16, 2002; parent U.S. Appl. No. 13/288,065.

A "Certificate of Existence" Bright Idea Inventor, LLC. Nov. 6, 2002; parent U.S. Appl. No. 13/288,065.

Operating Agreement of Bright Idea Inventor, LLC received from Pfeiffer & Gantt, PA, dated Nov. 13, 2002; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Congressman from Maryland, Elijah E. Cummings, dated Dec. 16, 2002; parent U.S. Appl. No. 13/288,065.

A newspaper article of Mr. Melvin Sullivan and Mr. Larry Golden, dated, Feb. 27-Mar. 5, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated May 21, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Office of the Vice President, Dick Cheney, dated Jun. 3, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated Oct. 1, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Lindsey O. Graham, dated Oct. 21, 2003; parent U.S. Appl. No. 13/288,065.

A letter sent to the President of the United States George W Bush, the President's Cabinet, the United States Senate and the Congressional Black Caucus, dated May 23, 2005; parent U.S. Appl. No. 13/288,065.

On Nov. 17, 2005, an "Inventor's Official Record of Invention", was filed in my name (Golden) at "The Law Office of David P. Gaudio, P.C.; the Inventors Network."; parent U.S. Appl. No. 13/288,065.

On Aug. 23, 2005, the "Disclosure Document Registration"; parent U.S. Appl. No. 13/288,065.

On Apr. 5, 2006, the "Patent Application" was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; parent U.S. Appl. No. 13/288,065.

On Jun. 6, 2008, the "Continuance-In-Part, (CIP) Application" was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; parent U.S. Appl. No. 13/288,065.

On Jan. 20, 2010, a "Continuation Application" (U.S. Appl. No. 12/657,356) was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; parent U.S. Appl. No. 13/288,065.

Reissue of U.S. Pat. No. 7,636,033; "Swear Back"; in accordance to Title 37—Code of Federal Regulations Patents, Trademarks, and Copyrights; Apr. 8, 2011; parent U.S. Appl. No. 13/288,065

Reissue of U.S. Pat. No. 7,636,033; "Swearback—History of Work"; Apr. 8, 2011; parent U.S. Appl. No. 13/288,065

United States Patent and Trademark Office; Office Action from U.S. 12/802,001; mailed Apr. 14, 2011; Alexandria, Virginia, USA; pp. 1-16; parent U.S. Appl. No. 13/288,065 (16 pages)

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; mailed Oct. 20, 2011; Alexandria, Virginia, USA; pp. 1-5; parent U.S. Appl. No. 13/288,065 (5 pages).

US 9,096,189 B2

Page 3

(56)

References Cited

OTHER PUBLICATIONS

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; mailed May 27, 2011; Alexandria, Virginia, USA; pp. 1-14; parent U.S. Appl. No. 13/288,065 (14 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802,001; copyright and mailing date Dec. 12, 2011, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Office Action, Office Action from U.S. Appl. No. 13/065,837; copyright and mailing date Dec. 2, 2011, pp. 1-27, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (27 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and mailing date Nov. 1, 2011, pp. 1-18, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (18 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/199,853; copyright and mailing date Jan. 13, 2012, pp. 1-34, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (34 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802,001; copyright and mailing date Mar. 26, 2012, pp. 1-12, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (12 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/199,853; copyright and mailing date Feb. 22, 2012, pp. 1-38, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (38 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and mailing date Feb. 22, 2012, pp. 1-25, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (25 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and mailing date Aug. 24, 2012, pp. 1-4, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (4 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and mailing date Nov. 28, 2012, pp. 1-11, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (11 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and mailing date Apr. 16, 2013, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (9 pages).

United States Department of Homeland Security; Petition for Inter Partes Review of U.S. Pat. No. Re. 43,990 Under 35 U.S.C. §312 and 37 C.F.R. §42.104; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-57; (57 pages).

United States Department of Homeland Security; Declaration of Dr. Sriram Vishwanath; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-44; (44 pages).

Richard R Brooks and S.S. Iyengar; Multi-Sensor Fusion Fundamentals and Applications with Software; published 1998; Copyright Prentice Hall PTR; Upper Saddle River, New Jersey, USA; pp. 1-20; (20 pages).

Ramanarayanan Viswanathan and Pramod K Varshney; Distributed Detection with Multiple Sensors; Part I—Fundamentals; Proceedings of the IEEE; Jan. 1, 1997; pp. 1-11; vol. 85; No. 1; Southern Illinois University Carbondale OpenSIUC; Illinois, USA; pp. 1-11; (11 pages).

Blum; Distributed with Multiple Sensors; Part II—Advanced Topics; Proceedings of the IEEE; Jan. 1, 1997; pp. 1-16; vol. 85, No. 1; Southern Illinois University Carbondale Open SIUC; Illinois, USA, pp. 1-11; (16 pages).

Victor Lesser; Distributed Sensor Networks a Multiagent Perspective; 2003; pp. 1, 2, 5, 6, 22, 26, 27, 36, 275, 320; copyright 2003 Kluwer Academic Publishers: AH Dordrecht, The Netherlands; (10 pages).

Samuel Blackman and Robert Popoli; Design and Analysis of Modern Tracking Systems; 1999; pp. 1, 2, 6, 472; copyright 1999 Artech House; Norwood, Massachusetts, USA; (4 pages).

Jean-Francois Chamberland; Decentralized Detection in Sensor Networks; 2003; pp. 407-416; IEEE Transactions on Signal Processing vol. 51, No. 2; Urbana, Illinois, USA; (10 pages).

Oleg Kachirski and Ratan Guha; Effective intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks; pp. 1-8; Proceedings of the 36th Hawaii International Conference on System Sciences; copyright 2003; Orlando, Florida, USA; (8 pages).

Lawrence A Klein; Sensor and Data Fusion a Tool for Information Assessment and Decision Making; 2004; pp. 1-4, 6, 81, 87-89; copyright 2004 The Society of Photo-Optical Instrumentation Engineers; Publisher is SPIE—the International Society for Optical Engineering; Bellingham, Washington, USA; (12 pages).

Dale Ferriere and Khrystyna Pysareva and Andrezej Rucinski; Using Technology to Bridge Maritime Security Gaps; Aug. 1, 2005; Sea Technology; pp. 1-6; copyright Compass Publications, Inc. Jan. 2009; Portsmouth, New Hampshire, USA; (6 pages).

Corie Lok; Cargo Security; MIT Technology Review; Jun. 2004; No. 107; pp. 74-75; publisher is Massachusetts Institute of Technology; Cambridge, Massachusetts, USA; (2 pages).

Thomas C Chen; RFID and Sensor-based Container Content Visibility and Seaport Monitoring system; Proceedings of SPIE, vol. 5778; pp. 151-159; Mar. 28, 2005; Publisher is SPIE—the International Society for Optical Engineering; Bellingham, Washington, USA; (10 pages).

United States Department of Homeland Security; The University of Texas at Austin College of Engineering Standard Resume of Sriram Vishwanath; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-21; (21 pages).

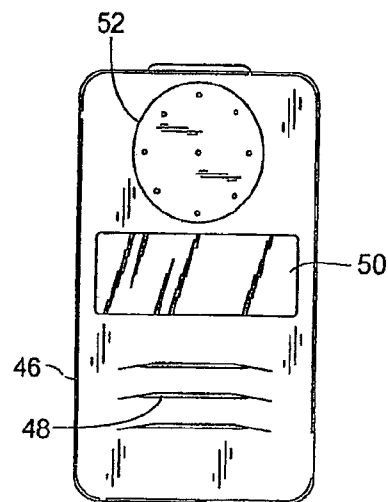
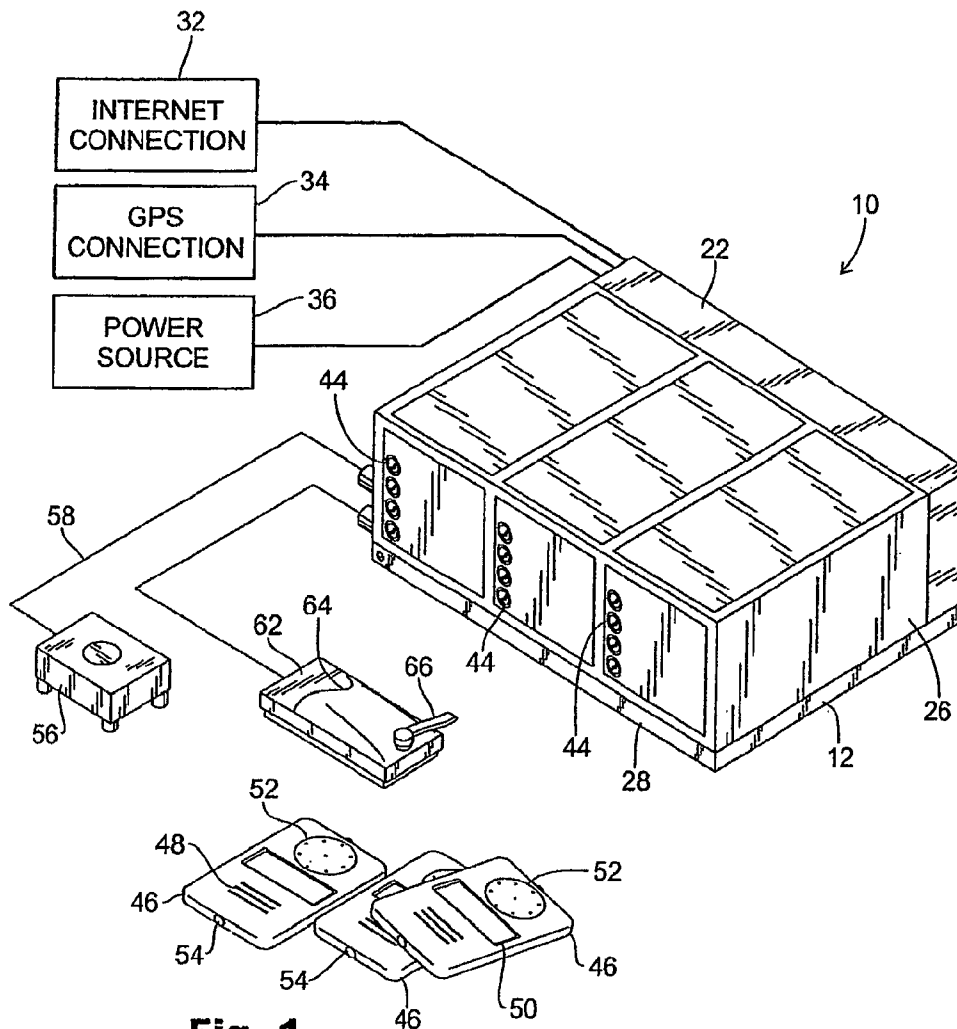
* cited by examiner

U.S. Patent

Aug. 4, 2015

Sheet 1 of 13

US 9,096,189 B2



U.S. Patent

Aug. 4, 2015

Sheet 2 of 13

US 9,096,189 B2

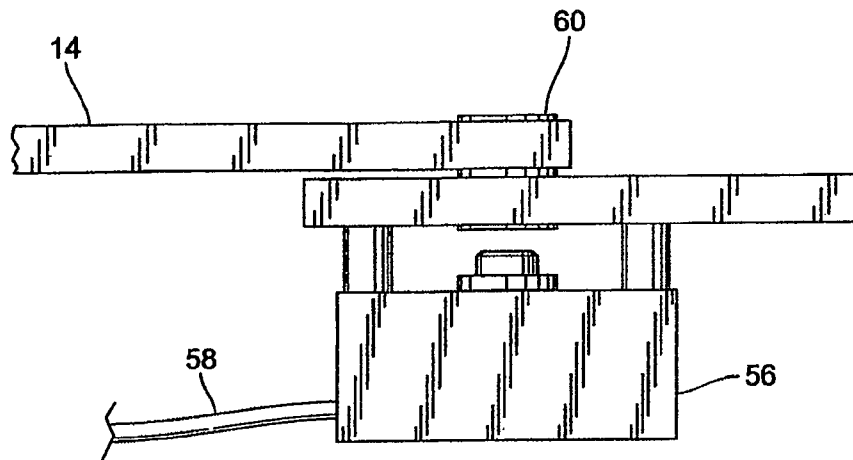


Fig. 3a

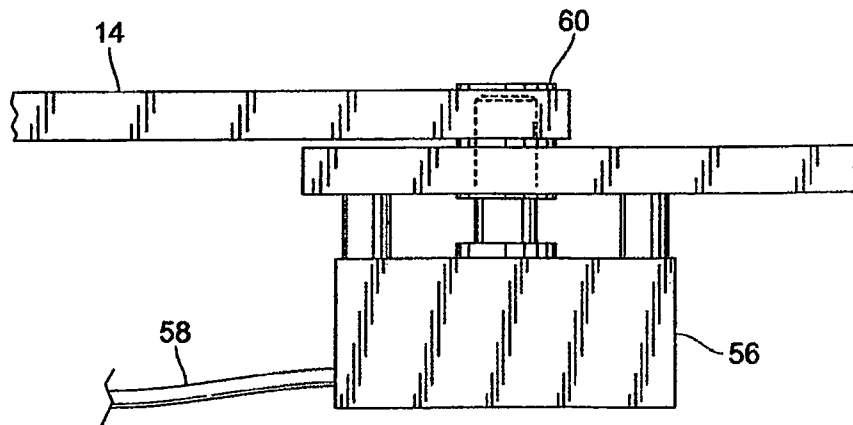


Fig. 3b

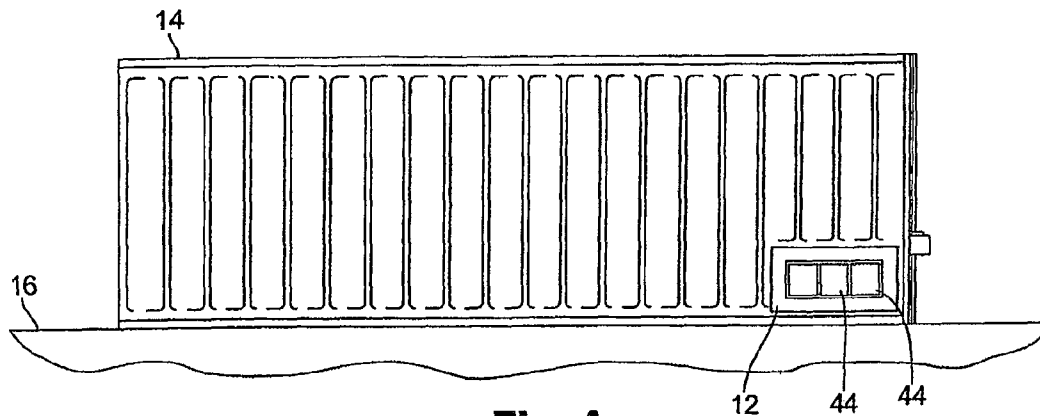


Fig. 4

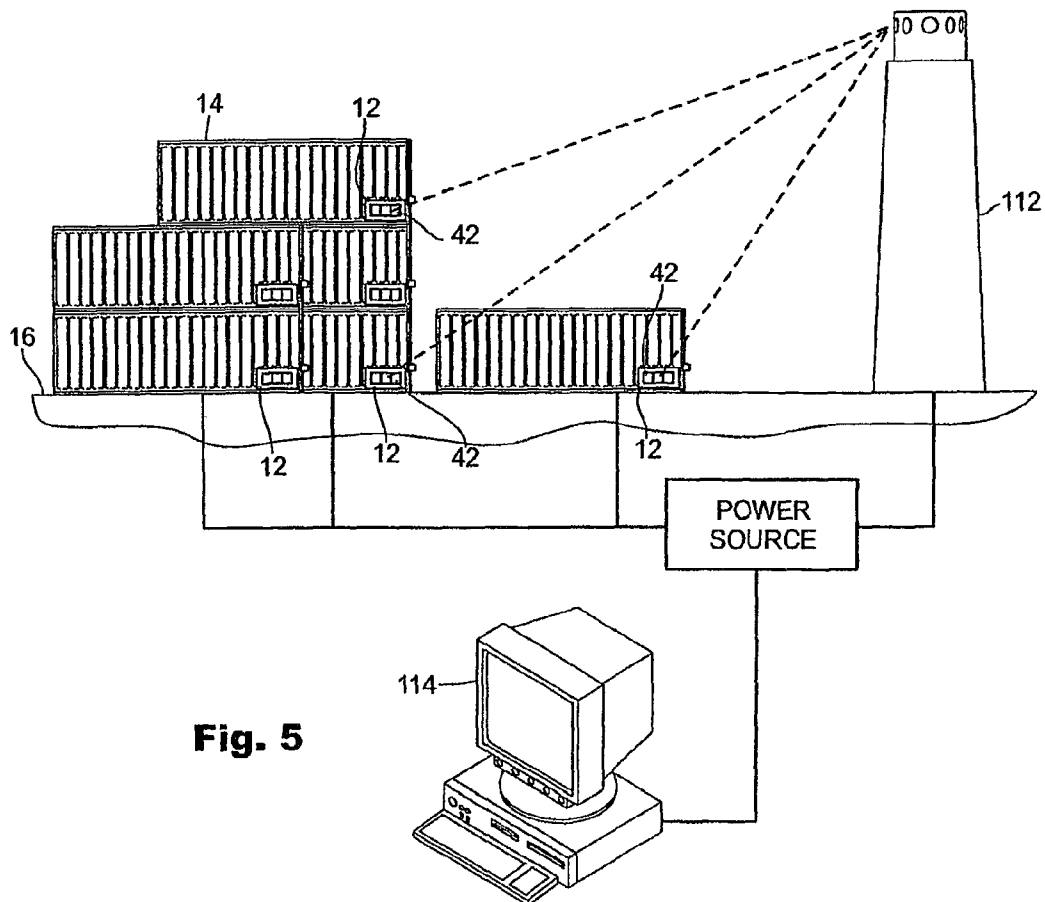
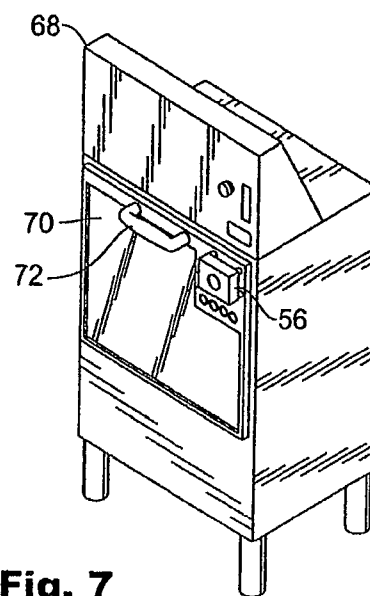
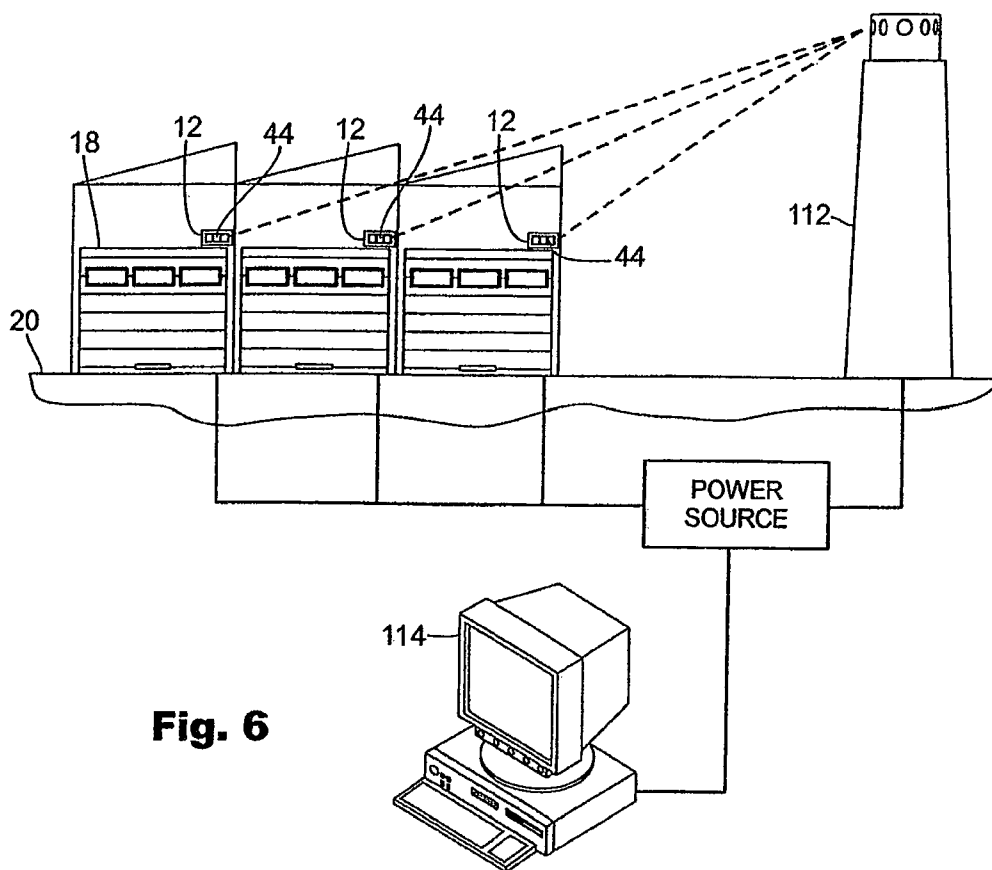


Fig. 5



U.S. Patent

Aug. 4, 2015

Sheet 5 of 13

US 9,096,189 B2

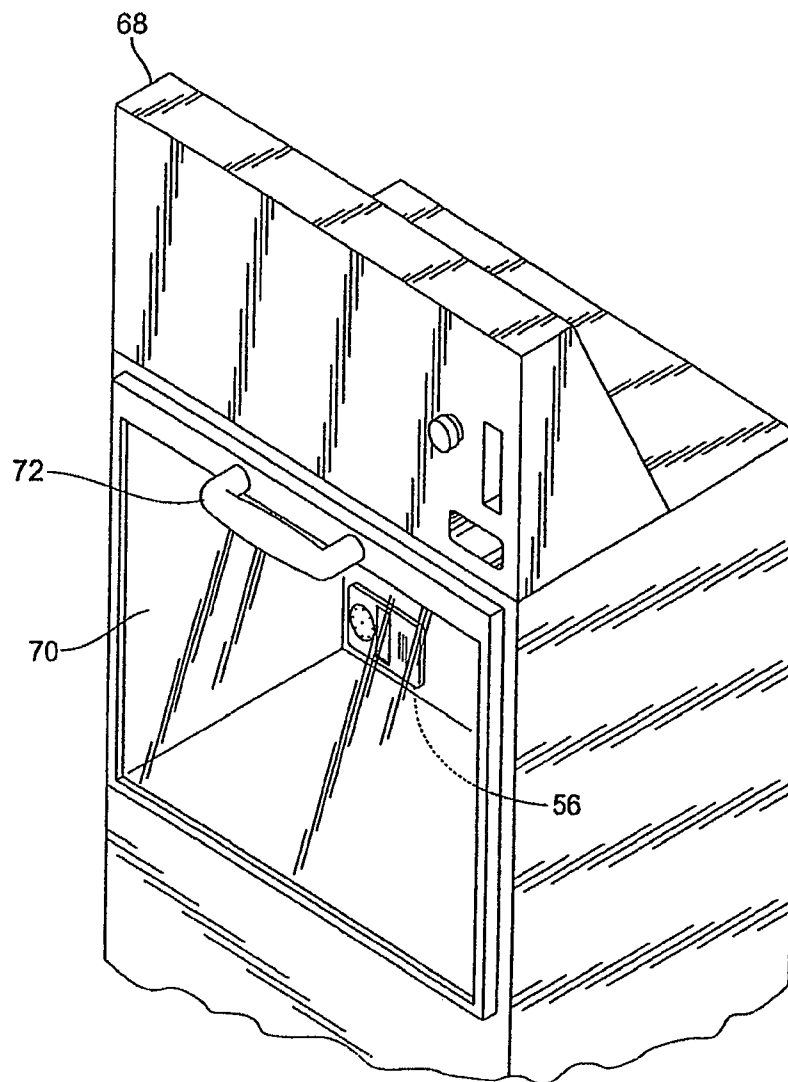


Fig. 8

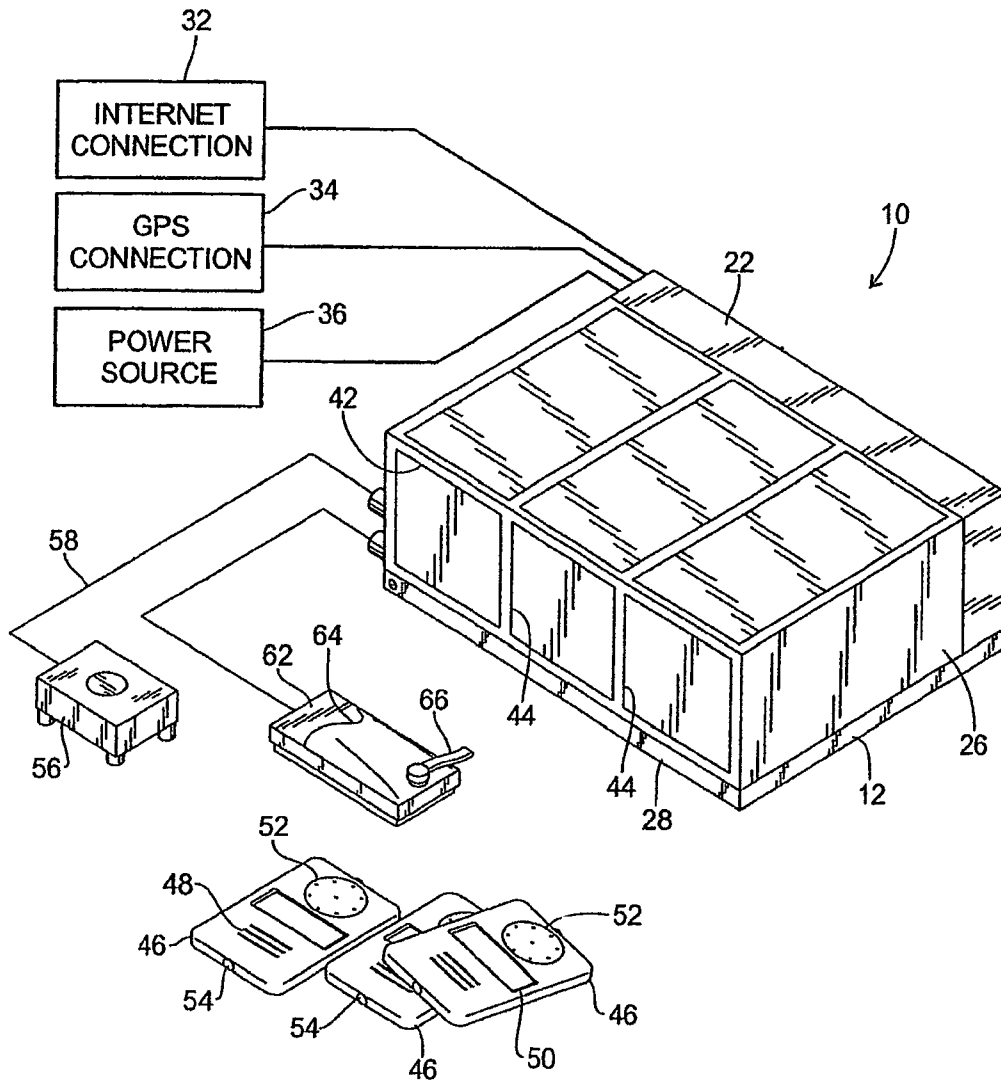


Fig. 9

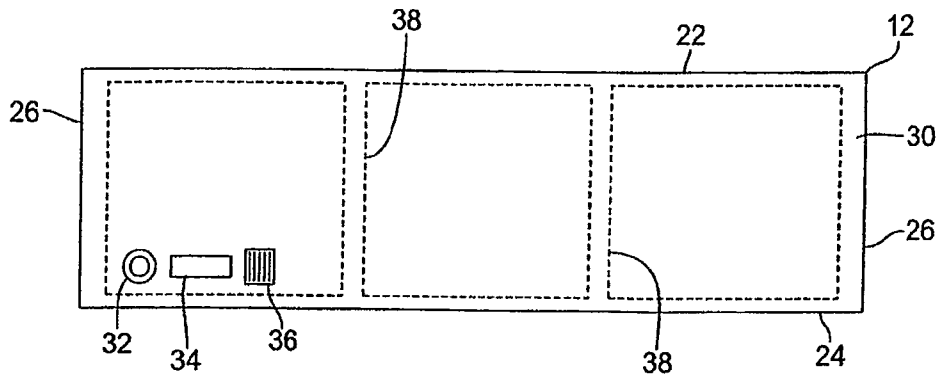


Fig. 10

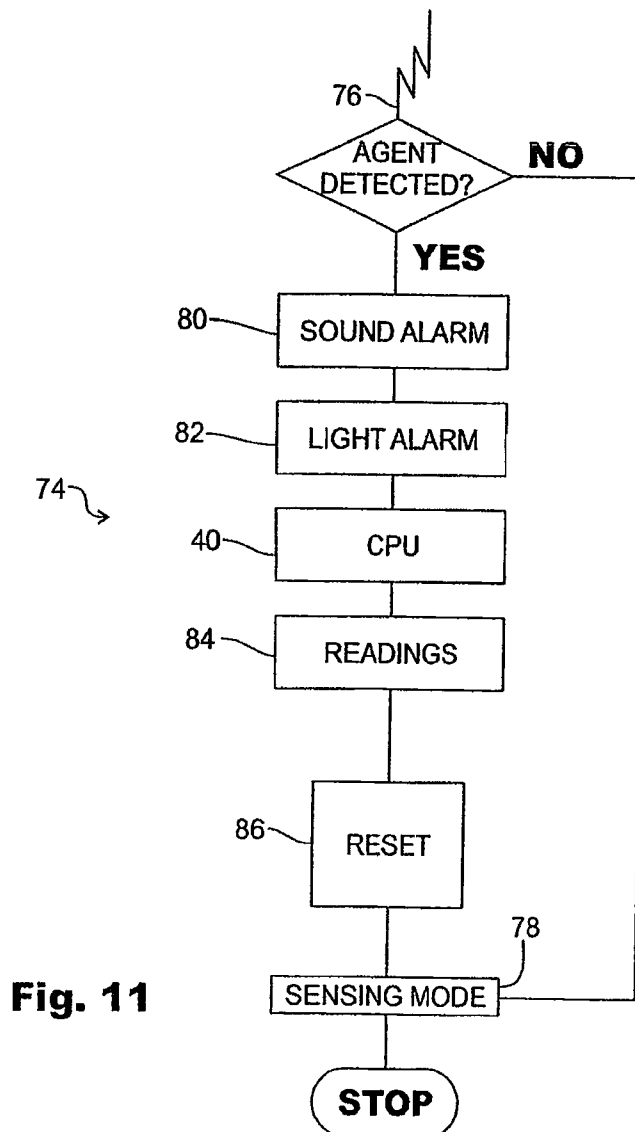


Fig. 11

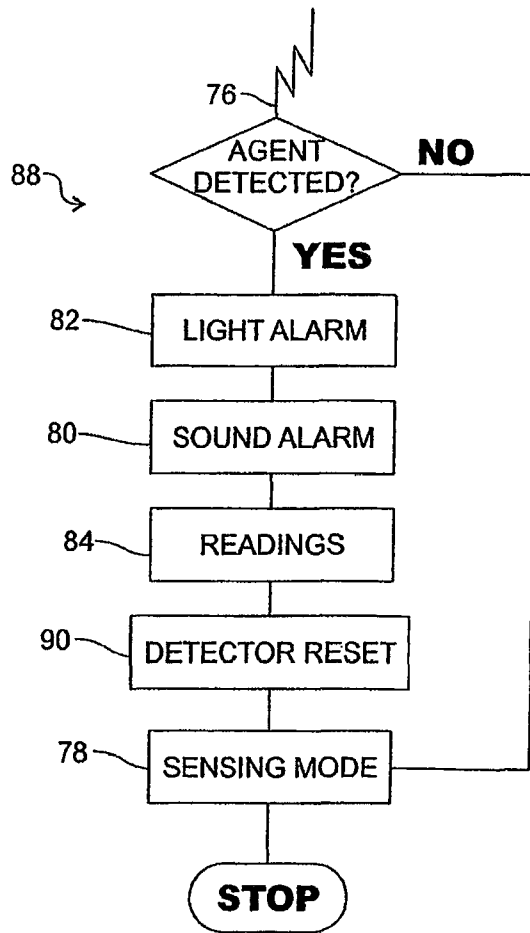


Fig. 12

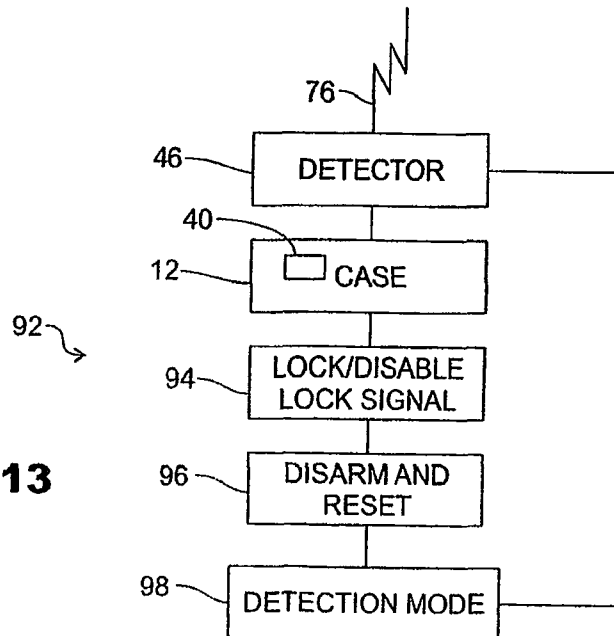


Fig. 13

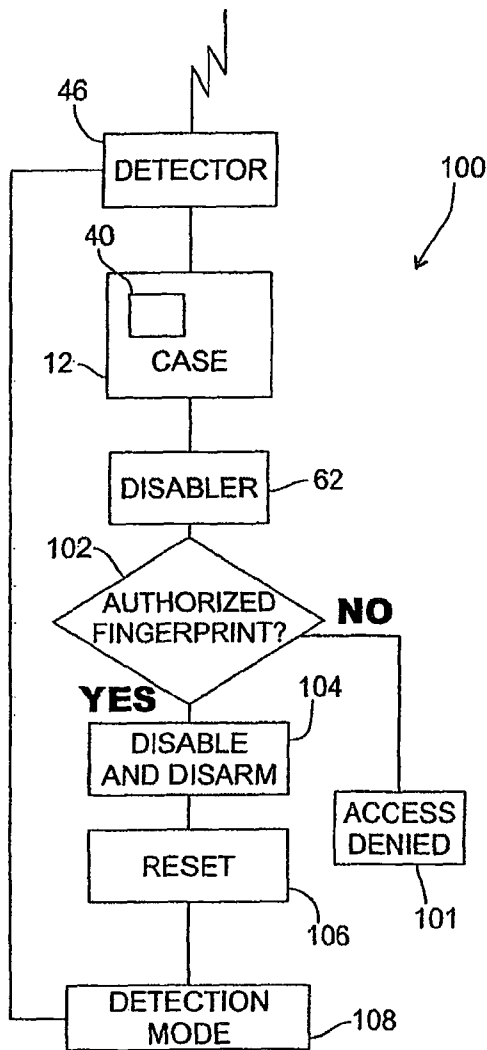


Fig. 14

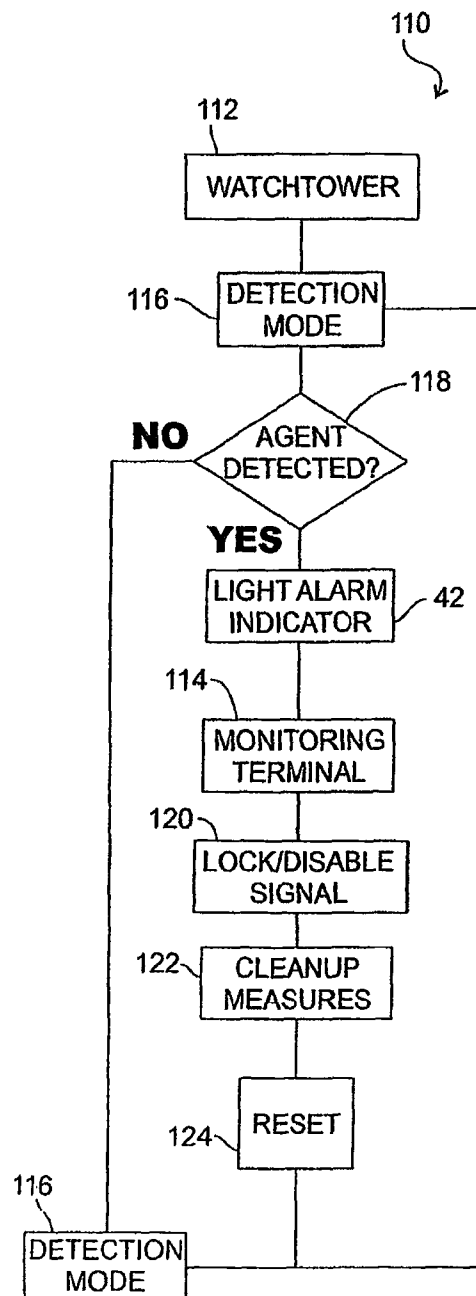


Fig. 15

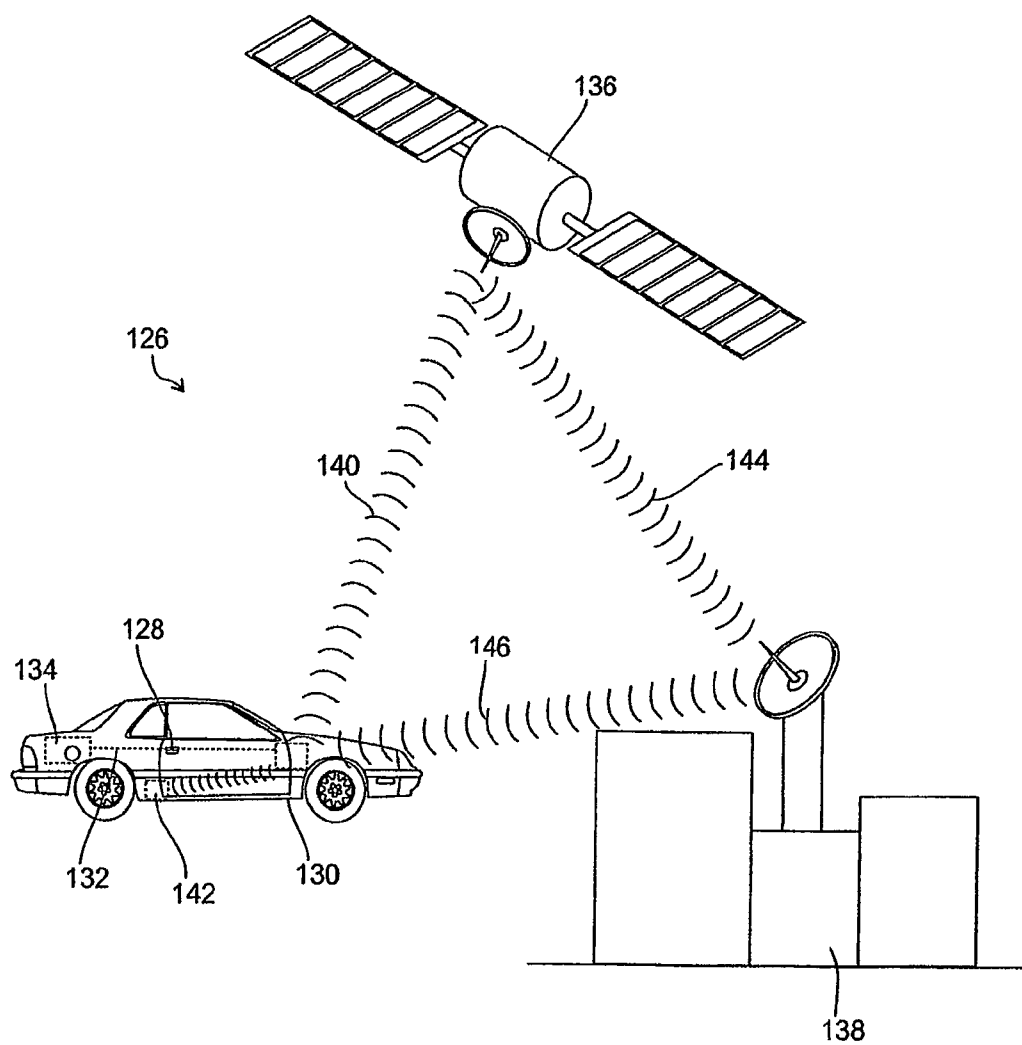


Fig. 16

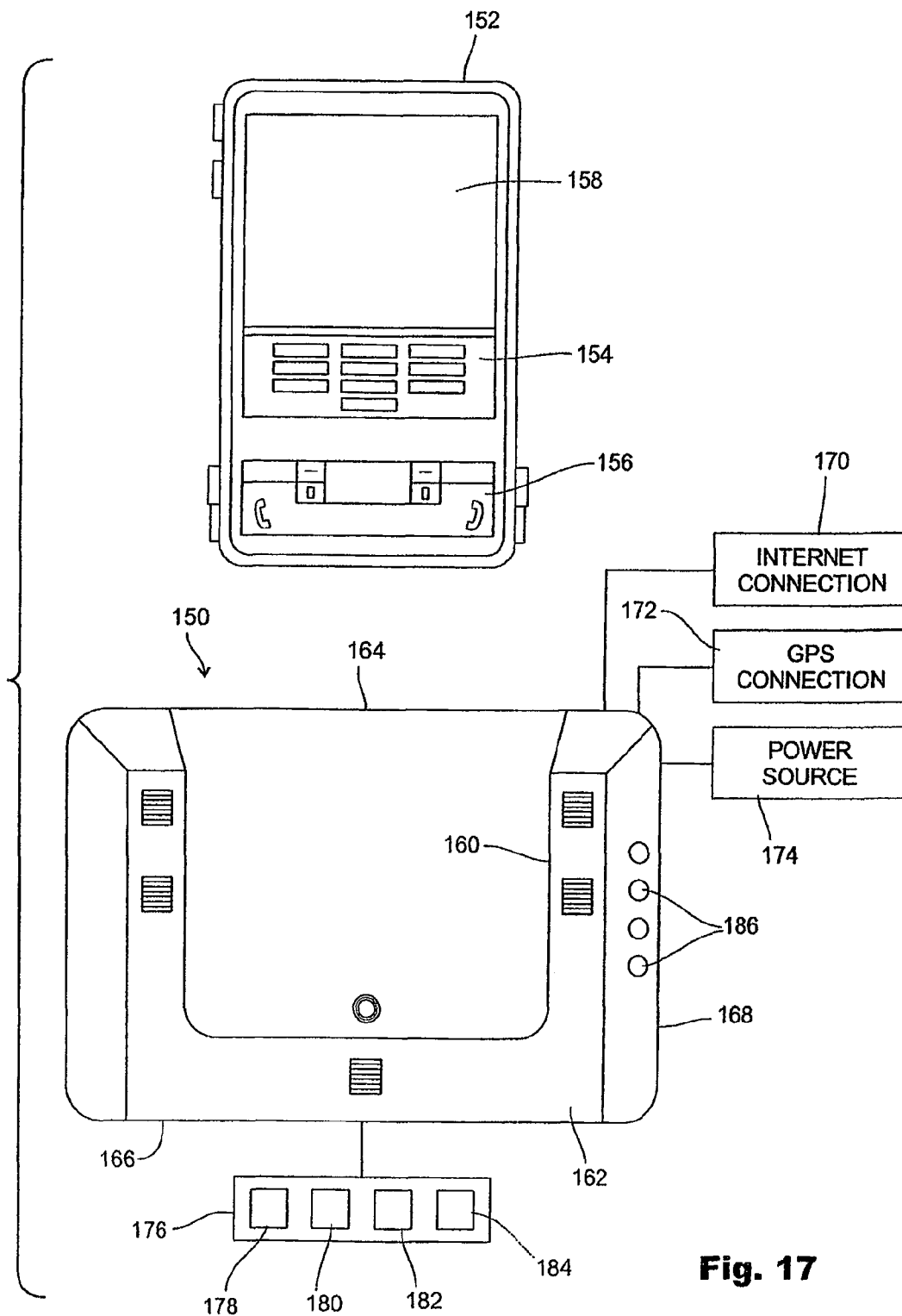


Fig. 17

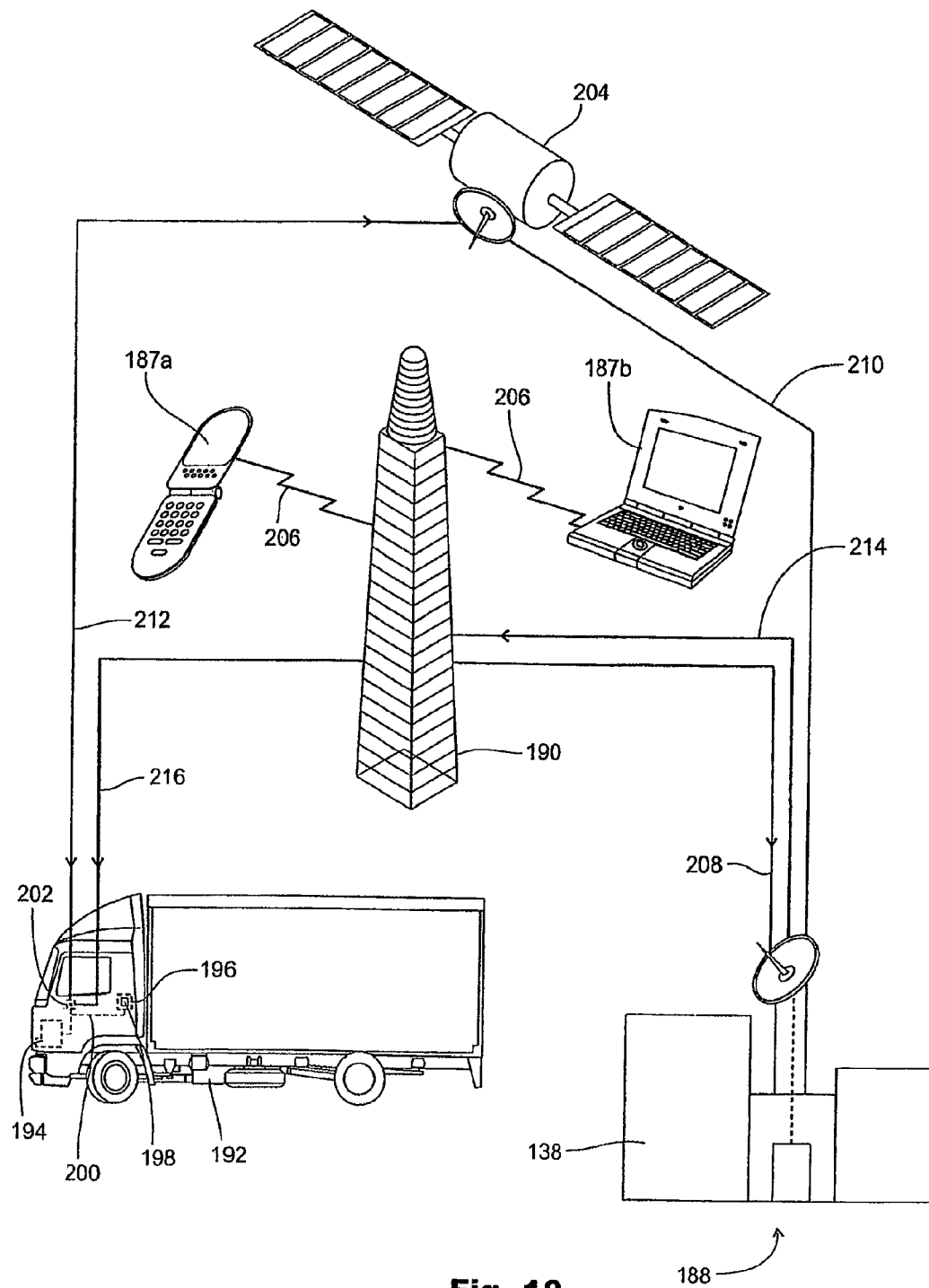


Fig. 18

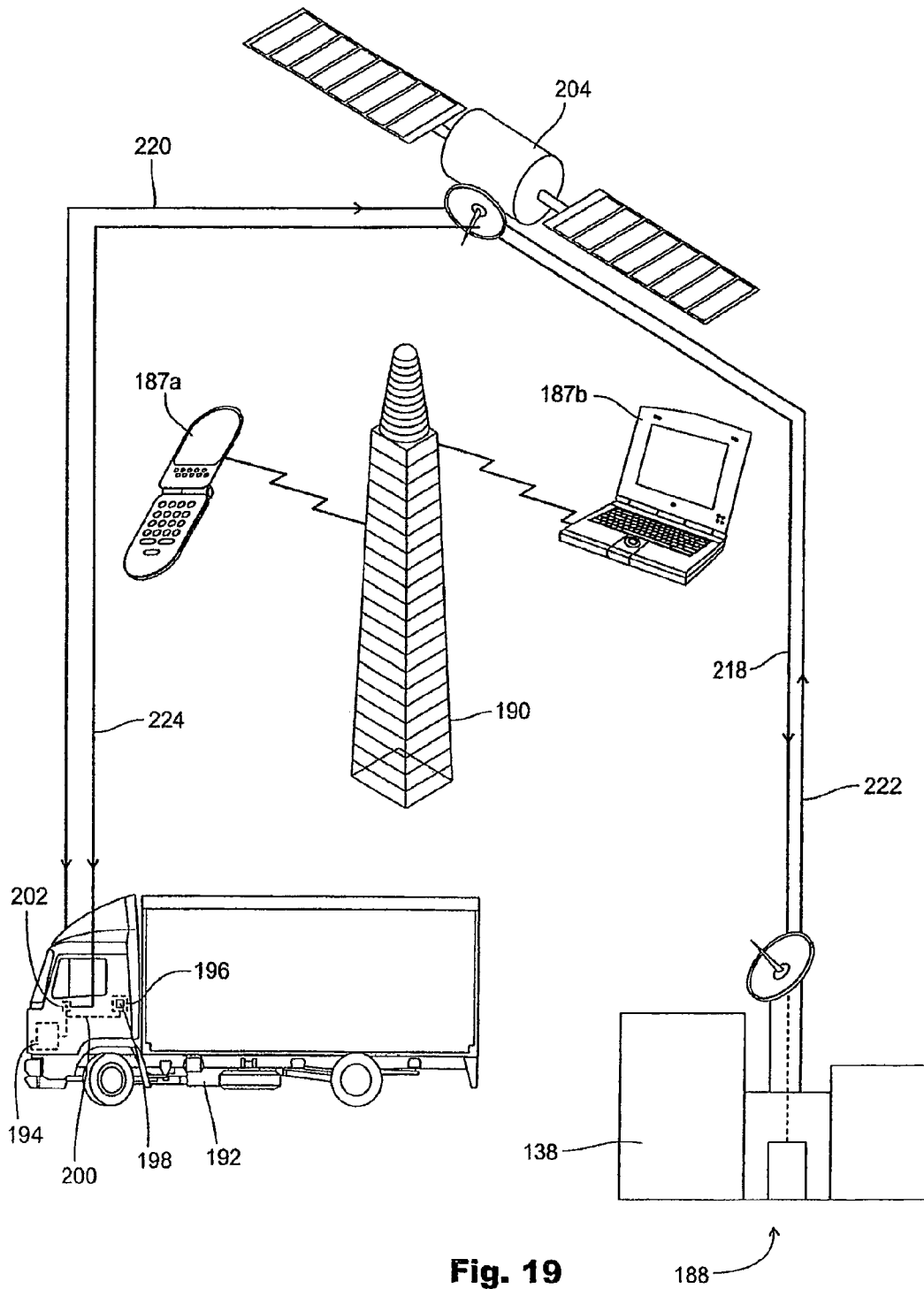


Fig. 19

US 9,096,189 B2

1

MULTI SENSOR DETECTION, STALL TO STOP AND LOCK DISABLING SYSTEM

This application is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 13/288,065 titled "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Nov. 3, 2011 and that will issue on Sep. 10, 2013 as U.S. Pat. No. 8,531,280, the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. patent application Ser. No. 13/288,065 that will issue as U.S. Pat. No. 8,531,280 is a divisional application and claims the filing date and benefit of U.S. patent application Ser. No. 12/802,001 titled "Multi Sensor Detection, Stall to Stop, and Lock Disabling System" filed on May 27, 2010, now U.S. Pat. No. 8,334,761, the entire contents and complete subject matter of which is incorporated by reference herein in their entirety for all purposes. U.S. patent application Ser. No. 12/802,001 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 12/657,356 titled "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Jan. 20, 2010, now U.S. Pat. No. 8,106,752 and incorporates the entire contents and complete subject matter therein by reference in their entirety for all purposes. U.S. patent application Ser. No. 13/288,065 that will issue as U.S. Pat. No. 8,531,280 also claims the filing date and benefit of and incorporates the entire contents of U.S. patent application Ser. No. 12/657,356, now U.S. Pat. No. 8,106,752 herein by reference for all purposes. The present application also claims the filing date and benefit of and incorporates the entire contents of U.S. patent application Ser. No. 12/802,001, now U.S. Pat. No. 8,334,761 by reference herein for all purposes. The present application also claims the filing date and benefit of and incorporates the entire contents of U.S. patent application Ser. No. 12/657,356, now U.S. Pat. No. 8,106,752 herein by reference for all purposes.

FIELD OF THE INVENTION

The present invention pertains to anti-terrorist detection and prevention systems, and more particularly pertains to a disabling lock mechanism combined with a chemical/biological/radiological detection system for use with products grouped together by similar characteristics in order to prevent unauthorized entry, contamination and terrorist activity.

BACKGROUND OF THE INVENTION

Terrorist activity is a continuous, daily, worldwide threat to the stability, prosperity, security and peace within nations and between and among nations. Its danger lies in its arbitrary destructiveness as much as in its unpredictability, and the constant threat of terrorist activity compels measures and actions that cause strain and contention in free, democratic societies as security concerns and civil liberty concerns must be balanced so that both public safety and civil liberties are maintained. Safety and security concerns can be addressed through numerous proactive steps and measures, many of which cause only minimal interference with and disruption of the daily routines of work, travel, commerce and entertainment. However, because modern industrial societies afford almost limitless places, locations, and opportunities for terrorist activities, no safety measure or security protocol will be foolproof, but many security measures, systems and protocols can be implemented that greatly minimize specific threats through fingerprint identification procedures, chemical, biological, and radiological hazard detections, bomb and

2

explosive detection, and controlling the access to everything from shipping containers to school lockers. Thus, the prior art discloses a wide range of security measures and systems.

For example, the Fishbine et al. patent (U.S. Pat. No. 4,792, 226) discloses an optical fingerprinting system that includes an optics/processor unit, a video monitor, a data terminal, and a printer for collecting and storing data characteristics of all ten individual fingerprints for printing demographic information and fingerprint images as desired on a standard booking or applicant card.

The Schiller patent (U.S. Pat. No. 4,544,267) discloses a finger identification unit that includes a fingerprint scanning apparatus using a collimated beam of light to interrogate the fingerprint of a finger placed against a platen so that successive scan positions produce signals containing fingerprint information.

The Fishbine et al. patent (U.S. Pat. No. 5,222,152) discloses a portable fingerprint scanning apparatus for optically scanning and recording fingerprint images and wirelessly transmitting such images to a mobile processing unit for verification and background checking.

The Loughheed et al. patent (U.S. Pat. No. 5,233,404) discloses an optical scanning apparatus that uses a linear charge coupled device (CCD) for recording the image of a fingerprint on the viewing surface.

The Groger et al. patent (U.S. Pat. No. 5,766,956) discloses a diode laser based sensor for undertaking optical, chemical, immunological or nucleic acid-based assay or other chemical analysis.

The Feldman patent (U.S. Pat. No. 5,938,706) discloses a multi element security system for preventing the unauthorized use of an automotive vehicle, and which includes numerous locking and control features interconnected to an onboard cpu.

The Bowker et al. patent (U.S. Pat. No. 5,963,657) discloses a safety access control for doors, handles, locks, etc., wherein the surface relief of a finger is read and verified to either allow or prevent access by the individual to the door, handle, lock, etc.

The Bonder et al. patent (U.S. Pat. No. 6,078,265) discloses a fingerprint identification security system wherein a key lock operated security system utilizes the fingerprint of the individual to control user access to the security system, such as the ignition system of an automotive vehicle.

The Anzai et al. patent (U.S. Pat. No. 6,271,745 B1) discloses a keyless authorization system for use of a motor vehicle that includes fingerprint reading units located on the exterior or interior of the motor vehicle and which is coupled to a control unit for scanning, comparing and matching fingerprints to allow or disallow access to the motor vehicle.

The Hwang patent (U.S. Pat. No. 6,374,652 B1) discloses a fingerprint-activated doorknob in which a detecting sensor for a fingerprint is placed on the doorknob for measuring and searching the fingerprint against previously stored fingerprint inputs to control access to the door.

The Vor Keller et al. patent (U.S. Pat. No. 6,588,635 B2) discloses a safety holster for a firearm that includes a pivotally mounted retaining member and a fingerprint sensor for scanning fingerprint information so that only authorized users can withdraw the firearm from the holster.

The Cordery et al. patent (U.S. Pat. No. 6,613,571 B2) discloses a method and system for detecting biological and chemical hazards in the mail that includes sensors placed within the mail box for sampling and testing ambient air and so that mail can be safely transported through the mail system.

US 9,096,189 B2

3

The Nagata patent (U.S. Pat. No. 6,628,213 B2) discloses a coding method for digital signal coding and decoding that includes a CMI (code-marked inversion) method of signal coding.

Nonetheless, despite the ingenuity of the above devices, methods, and systems, there remains a need for a multi-detector and disabling lock system for use with various types of products collected together by common characteristics into product groupings for detecting chemical, biological and radiological agents and compounds and for selectively disabling and activating the product locks thereby preventing unauthorized entry and further contamination and preventing and thwarting terrorist activities.

SUMMARY OF THE INVENTION

The present invention comprehends a chemical/biological/radiological detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping 1 include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes and lockers; while the products grouped into what may be referred to as Product grouping 2 include, but are not limited to, chemical, biological, radiological, and nuclear detectors, motion sensors and door sensors. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

The multi sensor detection and lock disabling system includes a detector case sized to fit in, upon or adjacent any of the afordescribed products for detecting harmful and dangerous chemical, biological, and radiological agents, compounds and elements. In addition, the multi sensor detection and lock disabling system is capable of transmitting a signal to lock or disable a lock on the product, and is also capable of transmitting signals to a monitoring computer terminal or PC so that appropriate defensive and safeguarding actions can be undertaken and an authorized individual can disarm and reset the locking system and the multi sensor detection system. The detector case includes a power source (battery or electrical), interior compartments, Internet and GPS connections and a cpu interconnected with the Internet and GPS connections, and also interconnected with one or more off site monitoring computer terminals or PCs. The detector case includes one or more light alarm indicators that are externally visible and that light up when the chemical, biological, or radiological agent or compound is detected, and the light alarm indicators (which can be indicator lights or panels on the front of the detector case) can be color coded for denoting the specific agent or compound detected, i.e., separate and distinct colors for indicating detection of the chemical, biological, or radiological agent or compound.

The detector case is designed to hold within the interior compartments one or more interchangeable detectors, and each detector is adapted and set up to sample a specific compound or agent. Each detector includes a sound alarm, a sensor, a light alarm, and a readings panel, and is electrically interconnected (either by wire or wirelessly) to the cpu of the detector case so that information regarding the detection of

4

the particular agent or compound can be conveyed from the detectors to the detector case cpu. Each detector can also be used as a manual, stand-alone hand held scanner.

The multi sensor detection and lock disabling system can be interconnected to a surveillance watchtower, as well as monitoring computer terminals or PCs, with the watchtower scanning shipping and cargo crates and containers being prepared for shipment or sitting for extended periods of time on a dock or at a port, at a railway site, or at an industrial storage facility. The watchtower will scan the cargo and shipping crates and containers for the light alarm indicators on detector cases that are mounted in or upon the crates and containers, and thus continuous security surveillance of the crates and containers can be maintained.

An enhanced version of the multi sensor detection and lock disabling system can be employed to prevent car and vehicle bombings. Coupling the multi sensor detection and lock disabling system with satellite service will enable the detection system to detect explosives and transmit an alert signal by satellite to monitoring equipment at a monitoring site. Upon receiving the alert signal at the monitoring site the monitoring equipment activates a stall-to-stop process for disabling the air, fuel, electrical and/or computer system of the vehicle. Moreover, upon receiving the alert signal at the monitoring site the car or vehicle will be locked by transmission of a satellite signal that disables the vehicle's electrical and ignition system thereby preventing escape of the terrorist.

It is an objective of the present invention to provide a multi sensor detection and disabling lock system for securing news racks and vending machines in order to prevent theft, unauthorized use and terrorist activity.

It is another objective of the present invention to provide a multi sensor detection and disabling lock system for preventing terrorist activity by using products grouped together by common features in several product groupings such as design similarity, similarity in the presentation of security problems and similarity with regard to the presentation of solutions to preventing terrorist solutions.

It is still yet another objective of the present invention to provide a multi sensor detection and disabling lock system that is capable of disabling an existing lock or activating a lock inside any of the products of the product grouping lists when a detector or sensor of the system is activated.

It is still yet a further objective of the present invention to provide a multi sensor detection and disabling lock system wherein the disabling lock system prevents the unauthorized entry, access and further contamination of the products included in the several product groupings.

A still further objective of the present invention is to provide a multi sensor detection and lock disabling system that utilizes a multi-task device for preventing terrorist activity to vulnerable products that are collected or arranged by product grouping categories.

Yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system to secure cargos and containers, especially cargo and shipping containers, against chemical, biological, radiological and nuclear terrorist activity.

Still another objective of the present invention is to provide a multi sensor detection and disabling lock system capable of detecting chemical, biological and radiological agents and compounds.

Still yet another objective of the present invention is to provide a multi sensor detection and disabling lock system that includes interchangeable detectors that operate in conjunction to detect chemical, biological and radiological agents and compounds.

US 9,096,189 B2

5

Still yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system that can be implemented by business or government at a minimum cost by organizing the products to be protected into product grouping categories.

Another objective of the present invention is to provide a multi sensor detection and disabling lock system that accurately and reliably detects harmful agents, compounds and elements, and prevents the placement and storage of weapons and bombs in the range of storage containers and facilities currently available.

Still another objective of the present invention is to provide a multi sensor detection and disabling lock system wherein the interchangeable detectors that comprise part of the system can be used as stand-alone scanners.

These and other objects, features, and advantages will become apparent to those skilled in the art upon a perusal of the following detailed description read in conjunction with the accompanying drawing figures and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the primary features of the system which include a detector case, several interchangeable detectors, an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler;

FIG. 2 is a front elevation view of the multi sensor detection and lock disabling system of the present invention illustrating one of the interchangeable detectors first shown in FIG. 1;

FIG. 3a is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one lock disabler to the lock of a product, such as a container, and disengaged from the lock of the container;

FIG. 3b is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the engagement of the lock disabler to the lock of the product for locking or disabling the lock of the product so that unauthorized access is prevented;

FIG. 4 is a side elevation view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case mounted to the product, such as the container, with the light alarm indicators externally visible;

FIG. 5 is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of detector cases with a surveillance watchtower and a monitoring PC terminal;

FIG. 6 is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the placement of detector cases upon containers different from the containers of FIG. 5, and wherein the detectors case are interconnected to a surveillance watchtower and a monitoring PC terminal;

FIG. 7 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one automatic/mechanical lock disabler to the lock of a standalone news rack;

FIG. 8 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating one interchangeable detector placed within the standalone news rack;

FIG. 9 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case having color coded front panels for specifically indicating the agents, compounds or elements that have been detected;

6

FIG. 10 is a rear elevation view of the multi sensor detection and lock disabling system of the present invention illustrating the GPS, Internet and power source connections;

FIG. 11 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector with the detector case and the steps undertaken by the system when an agent or compound is detected;

FIG. 12 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the sequence of steps undertaken by one detector when functioning as a standalone scanner for detecting an agent or compound;

FIG. 13 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector case with the automatic/mechanical lock disabler for activating the lock disabler upon detection by the system of an agent or compound;

FIG. 14 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating interconnection of the detector case with the fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public upon detection of the agent or compound;

FIG. 15 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the system with a surveillance watchtower and a monitoring PC or computer terminal for monitoring containers, such as shipping or cargo containers, that may sit for extended time periods on docks, at rail yards, and at industrial storage facilities;

FIG. 16 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the integration of the detection system with a satellite and monitoring equipment at a monitoring site for detecting explosives placed in a vehicle and then transmitting signals to the satellite and then to the monitoring site for disabling and locking the vehicle;

FIG. 17 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the features and elements of the detector case to a cell phone and cell phone case;

FIG. 18 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of a GPS satellite, a monitoring site and a cell phone tower for communicating to and with an electronic device such as a laptop computer or a cell phone for transmitting signals to a vehicle for activating an onboard stall-to-stop device for bringing the vehicle to a halt; and

FIG. 19 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the use of a GPS satellite in conjunction with the monitoring site and monitoring equipment to relay commands and signals to the cpu or transceiver of the vehicle for stopping or locking the vehicle in response to a signal that a certain type of event (detection of a bomb, engine failure or malfunction or unauthorized use) has occurred or is in process

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Illustrated in FIGS. 1-19 is a multi sensor detection and lock disabling system 10 for preventing terrorist activity by monitoring, detecting, and securing those critical areas, sites, and facilities vulnerable to terrorist activity. The first step is

US 9,096,189 B2

7

the identification of critical areas, sites, locations and facilities that are vulnerable to terrorist activity as convenient places to store and plant explosives and bombs and spread biological, chemical or radiological agents and compounds, followed by the disposition of the multi sensor detection and lock disabling system **10** for monitoring, detecting, and securing the particular location or site. Vulnerable sites, locations, facilities and areas are nearly limitless in their variety; in order to categorize the protection the present invention provides an anti-terrorist product grouping strategy has been developed wherein products made from the same or similar material, products having the same or similar design, and products presenting the same or similar security problems are grouped together with the multi sensor detection and lock disabling system **10** for preventing terrorist activity. For example, two preferred product groupings can be Product Grouping I: cargo containers, shipping containers, cargo planes, freight train cars, tractor trailers, mail carriers (UPS, FedEx), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans and utility vehicles. Product Grouping II: chemical detectors, biological detectors, radiological detectors, nuclear detectors, motion sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems. In addition to grouping products together by features, designs and materials, the multi sensor detection system **10** includes a lock disabling capability for disabling an existing lock or activating a lock on or inside any of the aforementioned products when a detector or sensor of the system is activated. The lock disabling feature is a crucial component of the invention in so far as it prevents unauthorized, unequipped or untrained individuals from gaining access and entry to the site and causing further contamination of the site.

As shown in FIGS. **1-10**, the multi sensor detection and lock disabling system **10** includes at least one—and preferably many—detector case **12** that can be placed in, on, upon or adjacent the product, such as the shipping containers **14** of FIGS. **4** and **5** resting upon a platform **16** or the cargo container **18** of FIG. **6** sitting upon a seaport dock or pier **20**. The detector case **12** includes a top **22**, a bottom **24**, a pair of opposed sides **26** and a front side or panel **28** and an opposite rear or back side **30**. The rear side **30** has connections or contacts that can include an Internet connection **32**, a GPS connection **34** and a power connection **36** for a power source. The power source for the detector system **10** can be any conventional battery or electrical source. The detector case **12** includes an interior chamber divided into a number of compartments **38** for holding therein agent or compound detection means hereinafter further described. A cpu **40** is mounted within the detector case **12** and electrically interconnects, routes, and transmits signals among items hereinafter further described and also communicates with a monitoring site and monitoring equipment. The front side **28** of the detector case **12** includes indicator means for visually indicating that a specific agent, compound or element has been detected. The indicator means can include color coded indicator lights **42** in panel form, as shown in FIG. **9**, with each indicator light panel **42** lighting up with a specific color corresponding to the detection of a specific agent or compound; or color coded indicator lights **44**, as shown FIG. **1**, that correspond to and individually light up on the detection of a specific agent or compound (chemical, biological, or radiological).

8

As shown in FIGS. **1**, **2** and **9-13**, the multi sensor detection and lock disabling system **10** includes a plurality of detectors **46** with each detector **46** adapted for and set up to sample for a specific agent or compound (biological, chemical, or radiological); and the detectors **46** are interchangeable for adapting to the needs and demands of future technology. The detectors **46** can also be used as standalone scanners. In the preferred embodiment of the invention, at least three detectors **46** are placed within the detector case **12** with one detector **46** specifically sampling biological agents or compounds, one detector **46** for sampling chemical agents or compounds, and one detector **46** for sampling radiological agents or compounds. The detectors **46** are interconnected to the cpu **40** of the detection system **10** by conventional connections that can be wire or wireless for transmitting the appropriate signals to the cpu **40** upon detection of the particular agent or compound. As shown in FIG. **2**, each detector **46** includes on its front plate or facing surface a sound alarm indicator **48**, a readings panel **50** comprising a plastic shield and LED lights for displaying the various read-out messages, a sensor **52** for detecting the specific agent, element or compound, and a light alarm indicator **54** that can be color coded for each specific agent and which is externally visible when the detector **46** is used as a stand alone scanner. Each detector **46** includes a conventional microprocessor for controlling the various functions and generating the appropriate signals for transmission to the cpu **40** of the detector case **12**.

As shown in FIGS. **1**, **3a**, **3b**, **9**, and **13-15**, used in conjunction with the multi sensor detection and lock disabling system **10** is at least one automatic/mechanical lock disabler **56**—and depending upon the number of products being monitored there can be one lock disabler **56** for each product. The automatic/mechanical lock disabler **56** is physically connected to the detector case **12** by a wire or cable **58** for receiving signals therefrom for disabling an existing lock or activating a lock inside a product to prevent access to the product. By way of example, FIG. **3a** shows the automatic/mechanical lock disabler **56** mounted—by any conventional means—to the lock **60** of the shipping container **14** shown in FIGS. **4** and **5** and connected by wire **58** to the cpu **40** of the detector case **12**. The lock disabler **56** is in the non-activated or disengaged state in FIG. **3a**. FIG. **3b** shows the automatic/mechanical lock disabler **56** mounted to the lock **60** of the shipping container **14** and in the activated or engaged state after detection of an agent or compound by the system **10** thereby for locking or disabling the lock **60** of the shipping container **14** and preventing unauthorized entry and access by unauthorized, untrained and unequipped individuals. In FIGS. **3a** and **3b** the lock **60** secures doors of the shipping container **14** that can be slidably or pivotably opened and closed.

In addition to the automatic/mechanical lock disabler **56**, the multi sensor detection and lock disabling system **10** can also utilize a fingerprint biometric lock with disabler **62** as shown in FIGS. **1** and **14**. The fingerprint biometric lock with disabler **62** is interconnected to the cpu **40** of the detector case **12** for receiving transmissions therefrom after detection of an agent or compound has occurred so that the lock on the product can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler **62** occurs when the fingerprint of the individual is placed on the fingerprint-matching pad **64**, and if a match occurs with a known fingerprint stored by the cpu **40**, then the individual can reset the fingerprint biometric lock with disabler **56** by turning the manual lock disabler **66**. The fingerprint biometric lock with disabler **62** is mounted to the lock of the product in a manner

US 9,096,189 B2

9

similar to the mounting of the automatic/mechanical lock disabler **56** that is shown in FIGS. **3** and **3b**.

FIGS. **4** and **5** show one manner of disposition or placement of the detector case **12** in relation to the product, i.e., the shipping container **14**, with the color coded indicator lights **42** externally viewable; FIG. **5** shows a number of shipping containers **14** each equipped with a detector case **12** and integrated with elements hereinafter further described for continuously monitoring the shipping containers **14** as they sit for an extended period of time on the truck or rail platform **16**. FIG. **6** illustrates several cargo containers **18** sitting on the shipping dock or pier **20**, with each cargo container **18** having a detector case **12** mounted thereon and integrated with and monitored by elements shown in FIG. **5** and hereinafter further described.

FIG. **7** illustrates a typical product from product grouping **1** that is monitored by the multi sensor detection and lock disabling system **10** of the present invention; specifically, FIG. **7** shows a news rack **68** with one automatic/mechanical lock disabler **56** mounted to and interconnected with the locking mechanism of the news rack **68**. As long as there is no detection of any agent or compound, the lock disabler **56** is in the disengaged state, and the individual can deposit the coin amount in the chute and then freely open the glass panel **70** by the handle **72** for removing a paper. However, the lock disabler **56** would be activated upon detection of the harmful agent or compound and receipt of a signal from the cpu **40** for locking or disabling the locking mechanism thereby denying access to the interior of the news rack **68** from all untrained, unauthorized and unequipped individuals.

FIG. **8** illustrates one detector **46** disposed within the news rack **68** and which is visible through the panel **70** for detecting one specific agent, compound or element. The detector **46** functions as a stand-alone scanner and can be wirelessly interconnected to offsite monitoring equipment.

FIG. **11** illustrates a representative schematic **74** for describing the signal transmission process from the detector **46** to the cpu **40** of the detector case **12**. The external stimulus **76** would be the chemical, biological or radiological agent or compound. If there is no detection of the agent or compound, the detector **46** will stay in the sensing mode **78**. However, detection of the specific agent will trigger the sound alarm **80** and the light alarm **82**, and instant transmittal of a signal to the cpu **40**. The readings **84** can be stored by the cpu **40** for verification and future review and evaluation. After all the appropriate corrective and preventative measures have been undertaken by the trained and authorized personal, and the site has been cleansed of the contamination, authorized and equipped personal can then reset **86** the system **10**.

FIG. **12** illustrates a representative schematic **88** for the detector **46** when used as stand-alone scanner. The detector **46** undergoes the same essential steps as illustrated in FIG. **11**, with the exception of the signal transmission to the cpu **40**. The detector **46** remains in detection mode **78** until an agent is detected, and then the various functions—light alarm **82**, sound alarm **80**, storage of readings **84**, and, after the appropriate security and safety steps have been carried out by authorized personal, detector reset **90** by authorized personal can occur thereby placing the detector **46** back in detection or sensing mode **78**.

FIG. **13** is a representative schematic **92** that illustrates the steps undertaken by the system **10** to lock or disable a lock, such as the lock **60** for the shipping container **14** shown in FIGS. **3a** and **3b**. Upon detection of the agent (chemical, biological, radiological) the alarm light indicators **42** or **44** will light up providing external indication that an agent has been detected. In addition, the system **10**—the cpu **40**—will

10

transmit a lock/disable lock signal **94** to the automatic/mechanical lock disabler **56** to lock or disable the lock on the product, such as the lock **60** on the shipping container **14** of FIGS. **3a-5**. This prevents unauthorized, unequipped, or untrained individuals from entering or gaining access to the product for which a dangerous and perhaps lethal agent has been detected. After the proper authorities and authorized personal have been notified and all the appropriate security, preventative and clean up measures have been undertaken, the authorized individual can perform the disarm and reset function **96** for the system **10** placing the system **10** in back in the detection mode **98**.

FIG. **14** is a representative schematic **100** illustrating the use of the fingerprint biometric lock with disabler **62** with the system **10**. Upon detection of the agent or compound by the detector, the various alarms would sound and light up (shown in previous figures), and the cpu **40** would then transmit a signal to the fingerprint biometric lock with disabler **62** to lock or disable the lock on the product, such as the lock **60** on the shipping containers **14** shown in FIGS. **3a-5**. The shipping containers **60** would remain locked and in an access denied mode **101** should an attempt be made to gain access to the container **60** by opening the lock **60** with an unauthorized fingerprint. However, a fingerprint that matches stored and authorized fingerprints **102** would indicate an authorized individual, and would allow the individual to disable and disarm **104** the lock **60** of the shipping container **14**. The fingerprint biometric lock with disabler **62** would then be reset **106** after the appropriate safety, cleanup, and protection measures are completed, and the system **10** would be reset and placed back in the detection mode **108**.

FIG. **15** is a schematic representation **110** that illustrates the integration of a surveillance watchtower **112** and a monitoring terminal or PC **114** for monitoring products such as the shipping containers **14** or cargo containers **16** that sit for extended periods of time of docks, piers **20**, truck terminals, mil yards, shipping platforms **16** and industrial sites as shown in FIGS. **5** and **6**. The watchtower **112** would maintain continuous surveillance over a number of shipping containers **60**, for example, with detector cases **12** mounted in or on each container **14** and set in detection mode **116** with one or more detectors **46** disposed in each detector case **12**. The watchtower **112** would continuously scan for light alarm indicators **42** and **44** on the products, such as the containers **14** or **18**, and the watchtower **112** would be interconnected and integrated with the monitoring terminal or PC **114**. Upon detection **118** of an agent or compound in one or more of the shipping containers **14**, the appropriate light alarm indicators **42** or **44** would light providing visible confirmation of the detection of the specific agent or compound. The cpu **40** would transmit a lock/disable signal **120** to the lock **60** on each respective shipping container **14** to lock or disable the lock **60** thus preventing access to that respective shipping container **14**. In addition, signal transmissions would be sent to the monitoring terminal or PC **114** (which could be off site) thereby alerting authorized security personal of the contamination event. With the information received at the monitoring terminal **114**, authorized personal would then be notified and dispatched to the area to undertake the appropriate safety and cleanup measures **122**. Such measures would also include disarming the lock disabling system in order to gain access to the shipping container **14**. After all the cleanup and security measures are completed by the trained and properly equipped authorities, the detection system and the lock disabling feature would reset **124** and the detection system would again be placed in detection mode **116**.

US 9,096,189 B2

11

FIG. 16 is a schematic representation 126 that illustrates an enhanced version of the multi sensor detection and lock disabling system 10 for preventing car and vehicle attacks and bombings. The lock disabling system 10 would be interconnected to the locking system and mechanism 128 of the vehicle 130. In addition, a stall to stop disabling link 132 can be made with the fuel, air, and electrical system 134 of the vehicle 130. The enhanced version incorporates a satellite 136 for signal receipt and transmission from the vehicle 130 in which the detector system 10 is placed to a monitoring site and monitoring equipment 138. As shown in FIG. 16, a detection signal 140 would be sent to the satellite 136 by the detection system 10 upon detection of a bomb or explosive 142 hidden in the vehicle 130. The satellite 136 would then transmit an alert signal 144 to the monitoring site 138 with the signal 144 containing the relevant data to evaluate the nature of the threat. The monitoring site 138 would then transmit a stall to stop signal 146 to the detection system 10 to lock the vehicle 130 and/or disable the electrical system of the vehicle 130 thereby disabling the vehicle 130, preventing access to the vehicle 130 by locking the vehicle 130, and preventing any terrorist in the vehicle 130 from escaping.

The detector case 12 can be modified and adapted for inclusion with cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, suitcases, and briefcases. In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring.

The system 10 and the watchtower 112, along with the satellite 136 and the monitoring site 138 can be adapted or incorporated with cell phone towers and satellites for use with satellite communication and/or a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu 40, a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween. The aforementioned telecommunication and radio communication means can be interactive with any type of motive vehicle that includes but is not limited to cars, trucks, vans, SUVs, trains, subways, boats, ships and airplanes, and which is reported stolen, experiences a loss of brakes, or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted to the vehicle and which detection causes an automatic signal transmission or a signal transmission is activated when a call is made to the monitoring station by an authorized person. The authorized individual includes but is not limited to the owner, pilot, conductor, captain, police highway patrol, security guard and military personnel to the monitoring equipment for activating a vehicle slowdown or stall-to-stop disabling system that similar to the disabling system 126 shown in FIG. 16, or incorporating features of the system 126 shown in FIG. 16, from the monitoring equipment to the vehicle. The activation of the stall-to-stop disabling means or the vehicle slowdown disables or engages the computer, electrical, fuel and air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to the brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.

In addition, the basic stall-to-stop disabling means or the vehicle slowdown means and device can be adapted, modified or designed to include: an open bust or open platform for integrating any new and innovative technology; warning lights indicators; sound alarm indicators; voice alarm indica-

12

tors; a cell phone to transmit to the vehicle a signal for slowing and halting the vehicle; and a lock disabling system or means to lock a thief or terrorist inside the vehicle after a transmission is received or sent. Open bust or open platform also refers to the compatibility of the detector case 12, or the incorporation of its features in cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, briefcases, and suitcases, etc., with other communication, transmission and surveillance systems whereupon the detector case 12, and its features, can be seamlessly integrated with other new and emerging systems and technologies.

Thus, as shown more specifically in FIG. 17, by way of a representative example the features and elements of the detector case 12 are shown as being incorporated into cell phone detector case 150 and associated cell phone monitor 152. The cell phone monitor 152 includes the standard keypad functions 154 and more specialized system use (ring tone, email, photos, texting) functions 156 as well as a viewing screen 158. The cell phone detector case 150 includes a recharging cradle or seat 160, a front side 162, a top 164, a bottom 166, and a pair of opposed sides 168. At the back of the cell phone detector case 150 are connections, contacts, and ports for at least an Internet connection 170, a GPS connection 172, and a contact, plug, or port for a power source 174. The power source for the cell phone detector case 150 can be any conventional rechargeable battery source or standard electrical power from a standard electrical receptacle or outlet.

As shown in FIG. 17, the cell phone detector case 150 includes one or more sensor/detector units, cells, or components 176 built into and incorporated into the case 150. The detector 176 includes generally disposed at the front 162 of the case 150 the following types of indicators: a sound alarm indicator 178, a readings panel 180, a sensor 182 for detecting one or more specific types of agents, elements, chemicals, compounds, etc., and a light alarm indicator 184. The sensor/detector 176 will be interconnected to the power source 174. In addition, mounted on and externally visible on the sides 168 or front 162 of the case 150 are a plurality of color coded indicator lights 186 with each light 186 corresponding to a specific agent, element, chemical, compound, etc., and lighting up when that agent is detected by the sensor/detector 176. The color coded indicator lights 186 will be electrically interconnected to the sensor/detectors 176 via any standard micro-processor. The cell phone detector case 150 and cell phone monitor 152 thus comprise a hand-held, easily portable and transportable detection means that is both effective and unobtrusive in its disposition and use.

FIGS. 18 and 19 illustrate representative examples of the integration of portable electronic communication or telecommunication devices such as a cell phone 187a and/or a laptop computer 187b with the monitoring equipment 138 located at a predesignated monitoring site 188, and operating in conjunction with either a satellite and/or a cell phone tower 190 to transmit and receive signals and commands among each other and to a vehicle 192, such as a truck, as part of a stall-to-stop disabling system for slowing and stopping the vehicle 192 and locking a thief, terrorist, or unauthorized individual in the vehicle 192 if needed. A wide range of events can trigger and initiate the stall-to-stop system and the locking or lock disabling system and mechanism, and the event doesn't have to be limited to the detection of a bomb or a chemical, biological, or radiological agent, element, or compound. The events can include, but is not limited to, detection of an engine problem to engine failure to the unauthorized use (stealing) of the vehicle 192. The vehicle 192 includes an electromotive system 194 that comprises, among other com-

US 9,096,189 B2

13

ponents, an onboard computer(s), electrical, fuel and air systems, as well as brakes, ignition, steering, and transmission. Also integrated with and capable of communicating with the vehicle's 192 electromotive system 194 is a stall-to-stop system while a lock disabling mechanism 196 is able to engage and disengage or disable the vehicle's 192 locking mechanism 198 upon receipt of the appropriate commands via a lock disabling communication channel or link 200. This link 200 can also accommodate the stall-to-stop system commands and signals, and thus is a multi-channel communication link. A CPU or a transceiver 202 is programmed to receive signals from the cell phone tower 190 and/or to a GPS satellite 204 and is interconnected with the stall-to-stop system and the lock disabling system 196 via link 200 for engaging the electromotive system 194 and actuating the lock disabling system 196 to stop the vehicle 192 and lock inside the vehicle 192 anyone such as a thief, terrorist or other unauthorized individual.

A representative example for stopping, disabling, and locking the vehicle 192 that utilizes the cell phone tower 190 wherein the activation and/or distress signal 206 originates from the cell phone 187a or the laptop 187b and such activation signal 206 travels to the cell phone tower 190 that is nearest the current location of the vehicle 192. A signal 208 is then transmitted to the monitoring site 188 and specific monitoring equipment 138 that can also include but is not limited to cell phones, laptops, desktop PC's, notebook PC's and LCD monitors. The monitoring site 138 then communicates by signal 210 to the GPS satellite 204 that an original or activation signal has been received and then the GPS satellite 204 locates and communicates by multiplex signal 212 with the CPU or transceiver 202 on the vehicle 192 and exchanges information on the type of problem, situation, location, and vehicle speed. The monitoring equipment 138 then transmits a signal 214 to the cell phone tower 190 that communicates with the transceiver 202 and/or CPU of the vehicle 192 to initiate or execute any commands that will actuate the stall-to-stop disabling link 200 and lock disabling system 196 for bringing the vehicle 192 to a halt and actuating the vehicle's 192 locking mechanism 198 for locking the thief, terrorist, or other unauthorized person inside the vehicle 192 if needed.

FIG. 19 illustrates a representative example wherein the stall-to-stop system and the lock disabling system 196 are utilized in conjunction with the GPS satellite 204. In FIG. 19 a signal has traveled to the satellites nearest the vehicle's 192 current location and then the signal 218 has traveled to the monitoring equipment 138 and monitoring site 188 which can include but is not limited to satellite cell phones, satellite monitors, cell phones, laptops, desktop PC's, notebook PC's, and LCD monitors. The GPS satellite 204 then locates and communicates with the CPU and/or transceiver 202 on the vehicle 192 via a multiplex (two-way) signal 220 in order to exchange information on such distress and danger event parameters as the specific problem situation, location, and vehicle speed. The monitoring equipment 138 then transmits a signal 222 back to the GPS satellite 204 that in turn communicates via another signal 224 with the CPU and/or transceiver 202 to execute any commands to the stall-to-stop system for executing the disengagement of the vehicle's 192 electromotive system 194 for bringing the vehicle 192 to a halt and for actuating the lock disabling system 196 to direct the lock disabling link 200 to actuate the locking mechanism 198 thereby locking the vehicle 192 and anyone inside the vehicle 192.

While the invention has been shown and described in a preferred embodiment, it will be apparent to those skilled in the art that numerous alterations, modifications, and varia-

14

tions will possible and practicable without departing from the spirit and scope of the invention as set forth by the appended claims.

The present invention comprehends a chemical/biological/radiological/nuclear/explosive/human/contraband detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars, (UPS, FedEx), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans, UAVs, UGVs, and utility vehicles; the products grouped into what may be referred to as Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, door sensors, speed sensors, biometric sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems, detection of humans, detection of contraband, temperature, and shock levels; the products grouped into what may be referred to as Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, suitcases, eyeglass, briefcases, detector cases of locks, detector cases of tags, detector cases that is mounted to, detector cases that is affixed to, detector cases that is outside of, detector cases that is inside of, and detector cases that is adjacent to; the products grouped into what may be referred to as Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, web servers, desktop PCs, notebook PCs, laptops, satellite cell phones, cell phones, UMTS phones, PDAs, LCD monitors, and satellite monitoring, remote control key fobs, two-way communication key fobs, handhelds; the products grouped into what may be referred to as Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Wi-Max, Internet, Ethernet, Broadband, Network Bandwidth, Wireless, Wired, Text Messaging, Cellular, Satellite, Telematics, Wide Area Network (WAN), Wireless Wide Area Network (WWAN), Local Area Network (LAN), Radio Frequency (RF), Broadband Wireless Access (BWA), Global Positioning System (GPS), General Packet Radio Services (GPRS), Global System for Mobile (GSM), Wideband Code Division Multiple Access (W-CDMA), Universal Mobile Telecommunications System (UMTS), Short Message Service (SMS); the products grouped into what may be referred to as Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature. the products grouped into what may be referred to as Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, HAZMAT, CIA, FBI, Secret Service, port security personnel,

US 9,096,189 B2

15

border security personnel, first responders, monitoring sites and terminal personnel. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside or outside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

The invention claimed is:

1. A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:

at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;

a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;

a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;

at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;

the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and

whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;

wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;

wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;

wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;

wherein the only type or types of communication with the transmitter and the receiver of the communication

16

device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).

2. Monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) interconnected to a product for communication therebetween, comprising:

at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;

a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;

a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;

a lock disabling mechanism that is able to engage (lock) and disengage (unlock) and disable (make unavailable) a product's lock, wherein the lock disabling mechanism disables the product's lock after a specific number of tries by an unauthorized user to disengage the lock by maintaining the product's lock in the current state of the product's lock regardless of input entered to change the state of the product's lock by the unauthorized user;

at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection, or GPS connection;

monitoring equipment of at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and

whereupon the monitoring equipment, is interconnected to a product equipped to receive signals from or send signals to the lock disabling mechanism that is able to engage and disengage or disable the lock, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;

wherein the monitoring equipment is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;

wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or long and short range radio frequency (RF) connection is in signal communication with the transmitter and the receiver of the monitoring equipment and transceivers of the products.

3. Monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) interconnected to a product for communication therebetween, comprising:

US 9,096,189 B2

17

at least one of a central processing unit (CPU), a network processor, or a microprocessor for executing and carrying out the instructions of a computer program or application which is specifically targeted at the networking application domain, for communication between the monitoring equipment and any of a plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container device, or a locking device;

a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container device, or a locking device;

a receiver for receiving signals, data or messages from at least one of plurality of product groups based on the categories of a multi-sensor detection device, a maritime cargo container device or a locking device, wherein the signals, data or messages are of agents of an item of interest (IOI);

at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or GPS connection;

the monitoring equipment is at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and

whereupon the monitoring equipment, is capable of the activation or deactivation of at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container device or a locking device;

wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, for signal communication with the transmitter and the receiver of the monitoring equipment and transceivers of the products;

at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of a chemical agent, a biological agent, a radiological agent, a nuclear agent, or an explosive agent which allows radio frequency (RF) data to be received and transferred between the tag and the monitoring equipment.

4. A built-in, embedded multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents;

comprising a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor;

comprising a communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a built-in sensor array or fixed detection device for communication therebetween,

wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the hand-

18

held, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;

wherein the built-in embedded multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories; and

wherein, when an alarm occurs, the built-in, embedded multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-long or short range radio frequency, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for communication therebetween;

wherein the built-in embedded multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity.

5. A built-in multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents, comprising:

a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor;

monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween;

wherein the built-in multi sensor detection device is built in any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);

wherein the built-in multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;

a light alarm indicator that has a plurality of colored lights that correspond to specific ones of the at least two agent;

wherein, when the light alarm indicator lights to indicate an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for the receipt and transmission of signals therebetween.

US 9,096,189 B2

19

6. A built-in multi sensor detection system for detecting at least two items selected from the group consisting of chemical agent, biological agent, radiological agent, explosive agent, human agent, contraband agent, motion, perimeter, temperature, tampering, theft, and breach, comprising:

a built-in sensor array or fixed detection device into a product that detects items by means of at least two sensors from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, and a radiological sensor;

monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween;

wherein the built-in, multi sensor detection device is built in any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);

wherein, when an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop) for the receipt and transmission of signals therebetween,

at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of the chemical agent, the biological agent, the radiological agent, the explosive agent, the human agent, the contraband agent, the motion, the perimeter, the temperature, the tampering, the theft, and the breach which allows radio frequency (RF) data to be received and transferred between the tag and the monitoring equipment.

7. A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:

a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds and capable of being disposed within, on, upon or adjacent a multi sensor detection device;

monitoring equipment comprising at least one of plurality product groups based on the categories of a computer, laptop, notebook, PC, handheld, cell phone, PDA or smart phone for the receipt and transmission of signals therebetween;

at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom or at least one satellite capable of transmitting signals to the monitoring equipment;

at least one satellite or at least one cell phone tower capable of signal communication between the multi sensor detection device and the monitoring equipment;

at least one internet connection capable of communication between the multi sensor detection device and the monitoring equipment;

20

whereupon a signal sent to a receiver of the multi sensor detection device from a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data;

wherein the monitoring equipment or multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;

wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the monitoring equipment or multi sensor detection device and transceivers of the products;

wherein the monitoring equipment is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the monitoring device that is at least one of the computer, the laptop, the notebook, the PC, the handheld, the cell phone, the PDA, or the smart phone is locked by the biometric lock disabler to prevent unauthorized use;

wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short range radio frequency (RF).

8. A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:

a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds and capable of being disposed within, on, upon or adjacent a multi sensor detection device;

monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween, wherein the monitoring equipment is equipped with a lock disabling mechanism that is able to engage (lock) and disengage (unlock) and disable (to make unavailable) a product's lock, wherein the lock disabling mechanism disables the product's lock after a specific number of tries by an unauthorized user to disengage the lock by maintaining the product's lock in the current state of the product's lock regardless of input entered to change the state of the product's lock by the unauthorized user;

at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom; or at least one satellite capable of transmitting signals to the monitoring equipment;

at least one satellite or at least one cell phone tower capable of signal communication between the multi sensor detection device and the monitoring equipment;

at least one internet connection capable of communication between the multi sensor detection device and the monitoring equipment; and

US 9,096,189 B2

21

whereupon a signal sent to a receiver of the multi sensor detection device from a satellite; or to a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data; 5

wherein the multi sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity; 10

wherein the multi sensor detection device for any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop); 15

wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or long and short range radio frequency (RF) connection is in signal communication with the transmitter and the receiver of the monitoring equipment or multi sensor detection device and transceivers of the products. 20

9. A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising: 25

a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds and capable of being disposed within, on, upon or adjacent a multi sensor detection device, wherein at least one of the sensors is capable of detecting agents of an item of interest (IOI); 30

monitoring equipment of at least one of the products grouped together by common features in the product groupings category of design similarity (i.e. computer 35

22

terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone) for the receipt and transmission of signals therebetween;

at least one satellite or at least one cell phone tower capable of signal communication between the multi sensor detection device and the monitoring equipment;

at least one internet connection capable of communication between the multi sensor detection device and the monitoring equipment;

whereupon a signal sent to a receiver of the multi sensor detection device from a satellite; or from a cell phone tower; or through short and/or long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data;

wherein the multi sensor detection device for any of one or more products listed in any of the plurality of product grouping categories to include but not limited to a maritime cargo container, a lock, or monitoring equipment (i.e., a computer terminal, personal computer (PC), a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop);

wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, or broadband connection, is in signal communication with the transmitter and the receiver of the monitoring equipment and transceivers of the products;

at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of the explosive agent, the nuclear agent, the contraband agent, the chemical agent, the biological agent, the human agent, or the radiological agent which allows radio frequency (RF) data to be received and transferred between the tag and the monitoring equipment.

* * * * *

(12) **United States Patent**
Golden

(10) **Patent No.:** **US 9,589,439 B2**

(45) **Date of Patent:** ***Mar. 7, 2017**

(54) **MULTI SENSOR DETECTION, STALL TO STOP AND LOCK DISABLING SYSTEM**

G08B 25/009; B60R 25/102; B60R 25/01; B60R 25/018; B60R 25/04; B60R 25/0405; B60R 25/0415; B60R 25/10

(71) Applicant: **Larry Golden**, Mauldin, SC (US)

See application file for complete search history.

(72) Inventor: **Larry Golden**, Mauldin, SC (US)

(56)

References Cited

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 81 days.

This patent is subject to a terminal disclaimer.

U.S. PATENT DOCUMENTS

4,385,469 A 5/1983 Scheuerpflug
4,544,267 A 10/1985 Schiller

(Continued)

OTHER PUBLICATIONS

(21) Appl. No.: **14/806,988**

(22) Filed: **Jul. 23, 2015**

(65) **Prior Publication Data**

US 2016/0027273 A1 Jan. 28, 2016

United States Department of Homeland Security; Petition for Inter Partes Review of U.S. Pat. No. Re. 43,990 Under 35 U.S.C. §312 and 37 C.F.R. §42.104; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-57; copy enclosed (57 pages)

(Continued)

Related U.S. Application Data

(60) Continuation of application No. 14/021,693, filed on Sep. 9, 2013, now Pat. No. 9,096,189, which is a
(Continued)

Primary Examiner — Van Trieu

(51) **Int. Cl.**

B60R 25/102 (2013.01)
G08B 13/24 (2006.01)
B60R 25/01 (2013.01)
B60R 25/04 (2013.01)
G07C 9/00 (2006.01)

(Continued)

(52) **U.S. Cl.**

CPC **G08B 13/2491** (2013.01); **B60R 25/018** (2013.01); **B60R 25/04** (2013.01); **B60R 25/102** (2013.01); **G07C 9/00912** (2013.01); **G08B 15/00** (2013.01); **G08B 21/12** (2013.01);

(Continued)

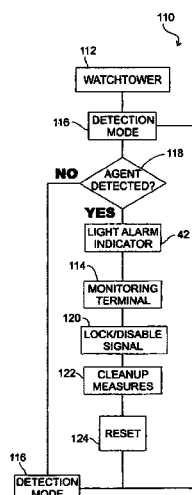
(58) **Field of Classification Search**

CPC G08B 15/00; G08B 15/001; G08B 15/004;

ABSTRACT

A multi sensor detection and disabling lock system includes detector cases for holding interchangeable detectors that sample for chemical, biological and radiological compounds, agents and elements, with each detector case disposed in or upon the monitored product. The detector case transmits detection information to a monitoring computer terminal and transmits a signal to a lock disabler engaged to the product to lock or disable the product's lock thereby preventing untrained, unauthorized and unequipped individual's from gaining access and entry to the product, and also preventing further contamination of the area. The detection system can be interconnected to surveillance towers scanning detector cases disposed at seaport docks, freight depots and rail terminals for monitoring containers being prepared for shipment or sitting on docks for long periods of time.

23 Claims, 13 Drawing Sheets



US 9,589,439 B2

Page 2

Related U.S. Application Data

continuation of application No. 13/288,065, filed on Nov. 3, 2011, now Pat. No. 8,531,280, which is a division of application No. 12/802,001, filed on May 27, 2010, now Pat. No. 8,334,761, which is a continuation of application No. 12/657,356, filed on Jan. 20, 2010, now Pat. No. 8,106,752, which is a continuation of application No. 12/155,573, filed on Jun. 6, 2008, now Pat. No. 7,636,033, which is a continuation-in-part of application No. 11/397,118, filed on Apr. 5, 2006, now Pat. No. 7,385,497.

(51) **Int. Cl.****G08B 15/00** (2006.01)**G08B 21/12** (2006.01)(52) **U.S. Cl.**

CPC ... *B60R 2325/205* (2013.01); *B60R 2325/304* (2013.01); *G07C 2009/0092* (2013.01)

(56)

References Cited

U.S. PATENT DOCUMENTS

4,586,441 A 5/1986 Zekich
 4,792,226 A 12/1988 Fishbine
 5,222,152 A 6/1993 Fishbine
 5,223,844 A 6/1993 Mansell et al.
 5,233,404 A 8/1993 Loughheed
 5,557,254 A 9/1996 Johnson
 5,682,133 A 10/1997 Johnson
 5,766,956 A 6/1998 Groger
 5,938,706 A 8/1999 Feldman
 5,959,529 A 9/1999 Kail, IV
 5,963,657 A 10/1999 Bowker
 5,986,543 A 11/1999 Johnson
 5,990,785 A 11/1999 Suda
 6,049,269 A 4/2000 Byrd
 6,078,265 A 6/2000 Bonder
 6,262,656 B1 7/2001 Byrd
 6,271,745 B1 8/2001 Arizal
 6,374,652 B1 4/2002 Hwang
 6,411,887 B1 6/2002 Martens
 6,470,260 B2 10/2002 Martens
 6,542,076 B1 4/2003 Joao
 6,542,077 B2 4/2003 Joao
 6,588,635 B2 7/2003 Vor Keller
 6,610,977 B2 8/2003 Megerie
 6,613,571 B2 9/2003 Cordery
 6,628,813 B2 9/2003 Scott
 6,647,328 B2 11/2003 Walker
 6,738,697 B2 5/2004 Breed
 6,923,509 B1 8/2005 Barnett
 6,980,092 B2 12/2005 Turnbull
 6,988,026 B2 1/2006 Breed et al.
 7,005,982 B1 2/2006 Frank
 7,034,677 B2 4/2006 Steintal et al.
 7,034,683 B2 4/2006 Ghazarian
 7,103,460 B1 9/2006 Breed
 7,109,859 B2 9/2006 Peeters
 7,116,798 B1 10/2006 Chawla
 7,148,484 B2 12/2006 Craig et al.
 7,164,117 B2 1/2007 Breed et al.
 7,171,312 B2 1/2007 Steintal et al.
 7,243,945 B2 7/2007 Breed et al.
 7,339,469 B2 3/2008 Braun
 7,346,439 B2 3/2008 Bodin
 7,385,497 B2 6/2008 Golden
 7,397,363 B2 7/2008 Joao
 7,636,033 B2 12/2009 Golden
 7,647,180 B2 1/2010 Breed
 7,844,505 B1 11/2010 Arneson et al.
 7,868,912 B2 1/2011 Venetianer et al.
 7,872,575 B2 1/2011 Tabe
 7,880,767 B2 2/2011 Chinigo

7,961,094 B2 6/2011 Breed
 8,274,377 B2 9/2012 Smith et al.
 8,531,521 B2 9/2013 Romanowich
 8,564,661 B2 10/2013 Lipton
 2002/0145666 A1 10/2002 Scaman
 2003/0063004 A1 4/2003 Anthony et al.
 2003/0137426 A1 7/2003 Anthony et al.
 2003/0206102 A1 11/2003 Joao
 2004/0107028 A1 6/2004 Catalano
 2004/0222092 A1 11/2004 Musho
 2005/0195069 A1 9/2005 Dunand
 2006/0164239 A1 7/2006 Loda
 2006/0176169 A1 8/2006 Doolin et al.
 2006/0181413 A1 8/2006 Mostov
 2006/0250235 A1 11/2006 Astrin
 2007/0171042 A1 7/2007 Metes et al.
 2008/0045156 A1 2/2008 Sakhpara
 2008/0122595 A1 5/2008 Yamamichi
 2008/0234907 A1 9/2008 Labuhn
 2010/0159983 A1 6/2010 Golden
 2011/0178655 A1 7/2011 Golden

OTHER PUBLICATIONS

United States Department of Homeland Security; Declaration of Dr. Sriram Vishwanath; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-44; copy enclosed (44 pages).
 Richard R Brooks and S.S. Iyengar; Multi-Sensor Fusion Fundamentals and Applications with Software; published 1998; Copyright Prentice Hall PTR; Upper Saddle River, New Jersey, USA; pp. 1-20; copy enclosed (20 pages).
 Ramanarayanan Viswanathan and Pramod K Varshney; Distributed Detection with Multiple Sensors: Part I—Fundamentals; Proceedings of the IEEE; Jan. 1, 1997; pp. 1-11; vol. 85; No. 1; Southern Illinois University Carbondale OpenSIUC; Illinois, USA; pp. 1-11; copy enclosed (11 pages).
 Blum; Distributed Detection with Multiple Sensors: Part II—Advanced Topics; Proceedings of the IEEE; Jan. 1, 1997; pp. 1-16; vol. 85, No. 1; Southern Illinois University Carbondale OpenSIUC; Illinois, USA; pp. 1-11; copy enclosed (16 pages).
 Victor Lesser; Distributed Sensor Networks a Multiagent Perspective; 2003; pp. 1, 2, 5, 6, 22, 26, 27, 36, 275, 320; copyright 2003 Kluwer Academic Publishers; AH Dordrecht, The Netherlands; copy enclosed (10 pages).
 Samuel Blackman and Robert Popoli; Design and Analysis of Modern Tracking Systems; 1999; pp. 1, 2, 6, 472; copyright 1999 Artech House; Norwood, Massachusetts, USA; copy enclosed (4 pages).
 Jean-Francois Chamberland; Decentralized Detection in Sensor Networks; 2003; pp. 407-416; IEEE Transactions on Signal Processing; vol. 51, No. 2; Urbana, Illinois, USA; copy enclosed (10 pages).
 Oleg Kachirski and Ratan Guha; Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks; pp. 1-8; Proceedings of the 36th Hawaii International Conference on System Sciences; copyright 2003; Orlando, Florida, USA; copy enclosed (8 pages).
 Lawrence A Klein; Sensor and Data Fusion A Tool for Information Assessment and Decision Making; 2004; pp. 1-4, 6, 81, 87-89; copyright 2004 The Society of Photo-Optical Instrumentation Engineers; Publisher is SPIE—the International Society for Optical Engineering; Bellingham, Washington, USA; copy enclosed (12 pages).
 Dale Ferriere and Khrystyna Pysareva and Andrzej Rucinski; Using Technology to Bridge Maritime Security Gaps; Aug. 1, 2005; Sea Technology; pp. 1-6; copyright Compass Publications, Inc. Jan. 2009; Portsmouth, New Hampshire, USA; copy enclosed (6 pages).
 Corie Lok; Cargo Security; MIT Technology Review; Jun. 2004; No. 107; pp. 74-75; publisher is Massachusetts Institute of Technology; Cambridge, Massachusetts, USA; copy enclosed (2 pages).
 Thomas C Chen; RFID and Sensor-based Container Content Visibility and Seaport Security Monitoring system; Proceedings of SPIE, vol. 5778; pp. 151-159; Mar. 28, 2005; Publisher is SPIE—

US 9,589,439 B2

Page 3

(56) **References Cited**

OTHER PUBLICATIONS

the International Society for Optical Engineering; Bellingham, Washington, USA; copy enclosed (10 pages).
United States Department of Homeland Security; The University of Texas at Austin College of Engineering Standard Resume of Sriram Vishwanath; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-21; copy enclosed (21 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 11/397,118; mailed Nov. 14, 2007; Alexandria, Virginia, USA; pp. 1-12; parent U.S. Appl. No. 13/288,065 (12 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/155,573; mailed Apr. 9, 2009; Alexandria, Virginia, USA; pp. 1-7; parent U.S. Appl. No. 13/288,065 (7 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/155,573; mailed Jul. 30, 2009; Alexandria, Virginia, USA; pp. 1-9; parent U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Notice of Allowability from U.S. Appl. No. 12/155,573; mailed Oct. 28, 2009; Alexandria, Virginia, USA; pp. 1-5; parent U.S. Appl. No. 13/288,065 (5 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/657,356; mailed Jul. 12, 2010; Alexandria, Virginia, USA; pp. 1-14; parent U.S. Appl. No. 13/288,065 (14 pages).

United States Patent and Trademark Office; Notice of Allowability from U.S. Appl. No. 12/657,356; mailed Mar. 10, 2011; Alexandria, Virginia, USA; pp. 1-4; parent U.S. Appl. No. 13/288,065 (4 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 13/065,837; mailed Jul. 18, 2011; Alexandria, Virginia, USA; pp. 1-9; parent U.S. Appl. No. 13/288,065 (4 pages).

A newspaper article of Mr. Melvin Sullivan and his family that references the date, Mar. 6, 2001; parent U.S. Appl. No. 13/288,065.

A letter of response Mr. Sullivan received from Pfeiffer & Gantt, PA, dated Sep. 16, 2002; parent U.S. Appl. No. 13/288,065.

A "Certificate of Existence" Bright Idea Inventor, LLC. Nov. 6, 2002; parent U.S. Appl. No. 13/288,065.

Operating Agreement of Bright Idea Inventor, LLC received from Pfeiffer & Gantt, PA, dated Nov. 13, 2002; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Congressman from Maryland, Elijah E. Cummings, dated Dec. 16, 2002; parent U.S. Appl. No. 13/288,065.

A newspaper article of Mr. Melvin Sullivan and Mr. Larry Golden, dated, Feb. 27-Mar. 5, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated May 21, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Office of the Vice President, Dick Cheney, dated Jun. 3, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated Oct. 1, 2003; parent U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Lindsey O. Graham, dated Oct. 21, 2003; parent U.S. Appl. No. 13/288,065.

A letter sent to the President of the United States George W. Bush, the President's Cabinet, the United States Senate and the Congressional Black Caucus, dated May 23, 2005; parent U.S. Appl. No. 13/288,065.

On Nov. 17, 2005, an "Inventor's Official Record of Invention", was filed in my name (Golden) at "The Law Office of David P. Gaudio, P.C.; the Inventors Network."; parent U.S. Appl. No. 13/288,065.

On Aug. 23, 2005, the "Disclosure Document Registration"; parent U.S. Appl. No. 13/288,065.

On Apr. 5, 2006, the "Patent Application" was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; parent U.S. Appl. No. 13/288,065.

On Jun. 6, 2008, the "Continuation-In-Part, (CIP) Application" was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; parent U.S. Appl. No. 13/288,065.

On Jan. 20, 2010, a "Continuation Application" (U.S. Appl. No. 12/657,356) was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; parent U.S. Appl. No. 13/288,065.

Reissue of U.S. Pat. No. 7,636,033; "Swear Back"; in accordance to Title 37—Code of Federal Regulations Patents, Trademarks, and Copyrights; Apr. 8, 2011; parent U.S. Appl. No. 13/288,065.

Reissue of U.S. Pat. No. 7,636,033; "Swearback—History of Work"; Apr. 8, 2011; parent U.S. Appl. No. 13/288,065.

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; mailed Apr. 14, 2011; Alexandria, Virginia, USA; pp. 1-16; parent U.S. Appl. No. 13/288,065 (16 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; mailed Oct. 20, 2011; Alexandria, Virginia, USA; pp. 1-5; parent U.S. Appl. No. 13/288,065 (5 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; mailed May 27, 2011; Alexandria, Virginia, USA; pp. 1-14; parent U.S. Appl. No. 13/288,065 (14 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802,001; copyright and mailing date Dec. 12, 2011, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and mailing date Dec. 2, 2011, pp. 1-27, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (27 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and mailing date Nov. 1, 2011, pp. 1-18, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (18 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/199,853; copyright and mailing date Jan. 13, 2012, pp. 1-34, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (34 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802,001; copyright and mailing date Mar. 26, 2012, pp. 1-12, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (12 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/199,853; copyright and mailing date Feb. 22, 2012, pp. 1-38, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (38 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and mailing date Feb. 22, 2012, pp. 1-25, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (25 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and mailing date Aug. 24, 2012, pp. 1-4, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (4 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and mailing date Nov. 28, 2012, pp. 1-11, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (11 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and mailing date Apr. 16, 2013, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright and mailing date Apr. 20, 2015, pp. 1-20, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 14/021,693 (20 pages).

US 9,589,439 B2

Page 4

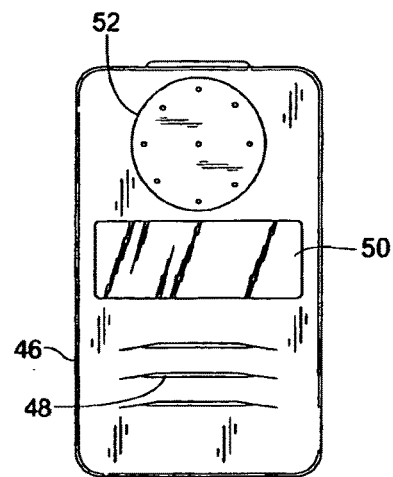
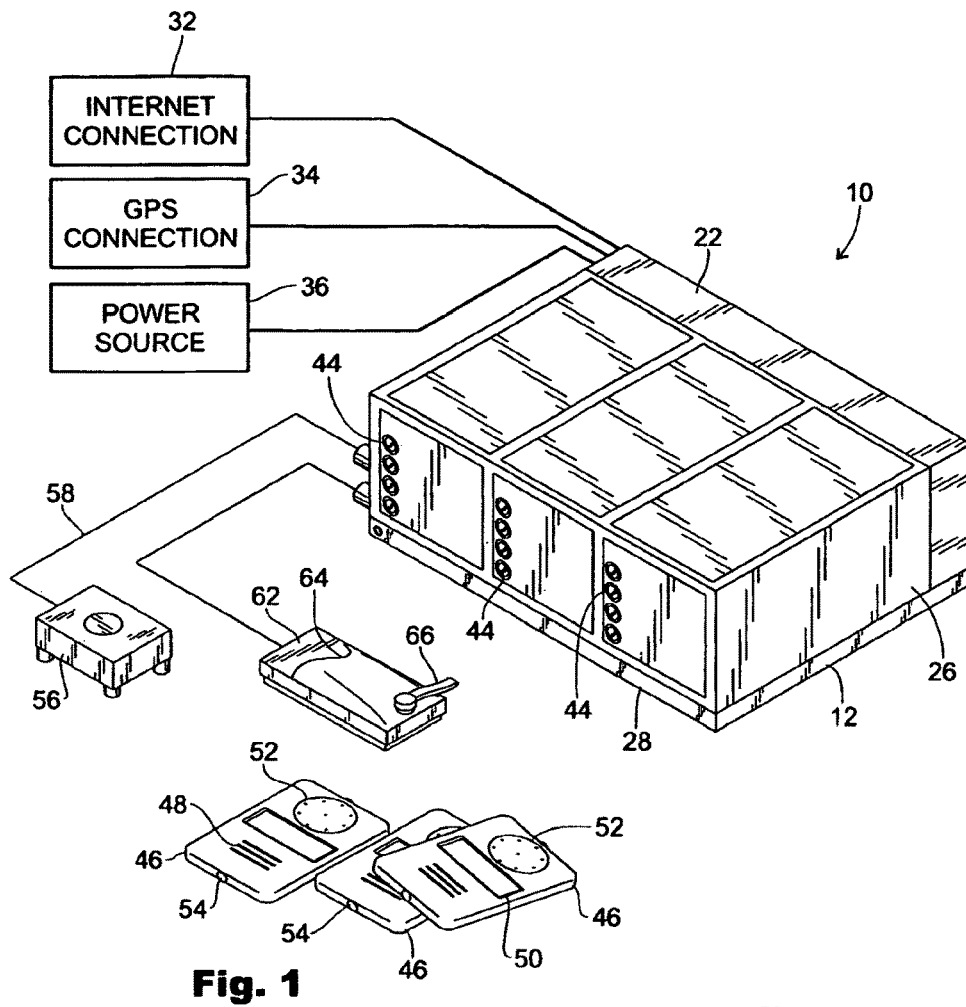
(56)

References Cited

OTHER PUBLICATIONS

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright and mailing date Jan. 20, 2015, pp. 1-17, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 14/021,693 (17 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright and mailing date Sep. 5, 2015, pp. 1-12, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 14/021,693 (12 pages).



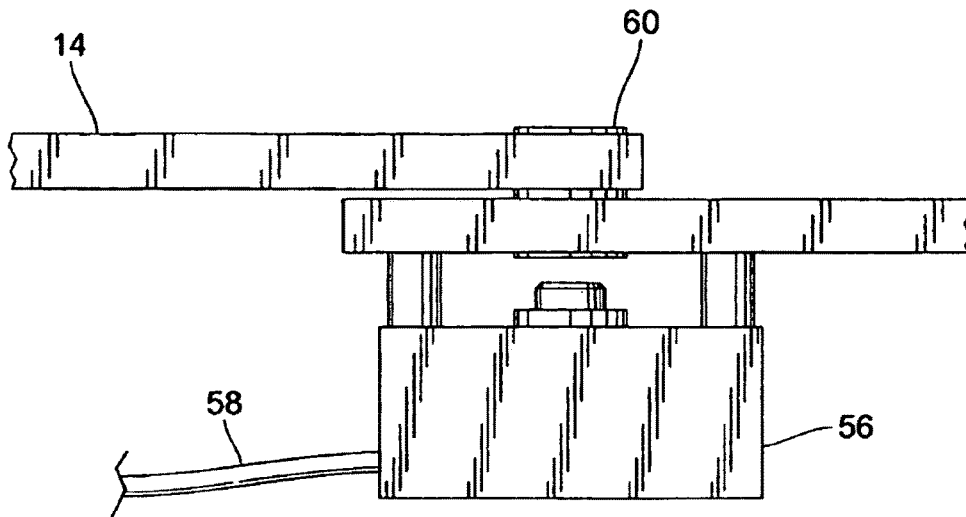


Fig. 3a

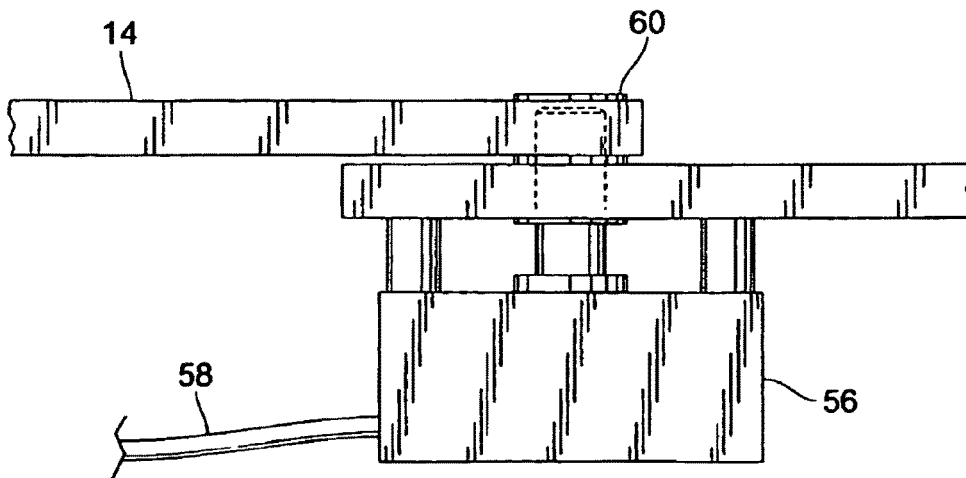


Fig. 3b

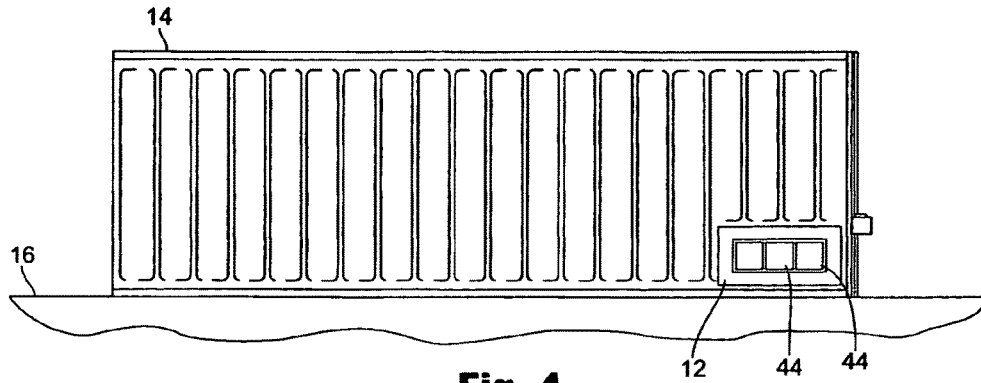


Fig. 4

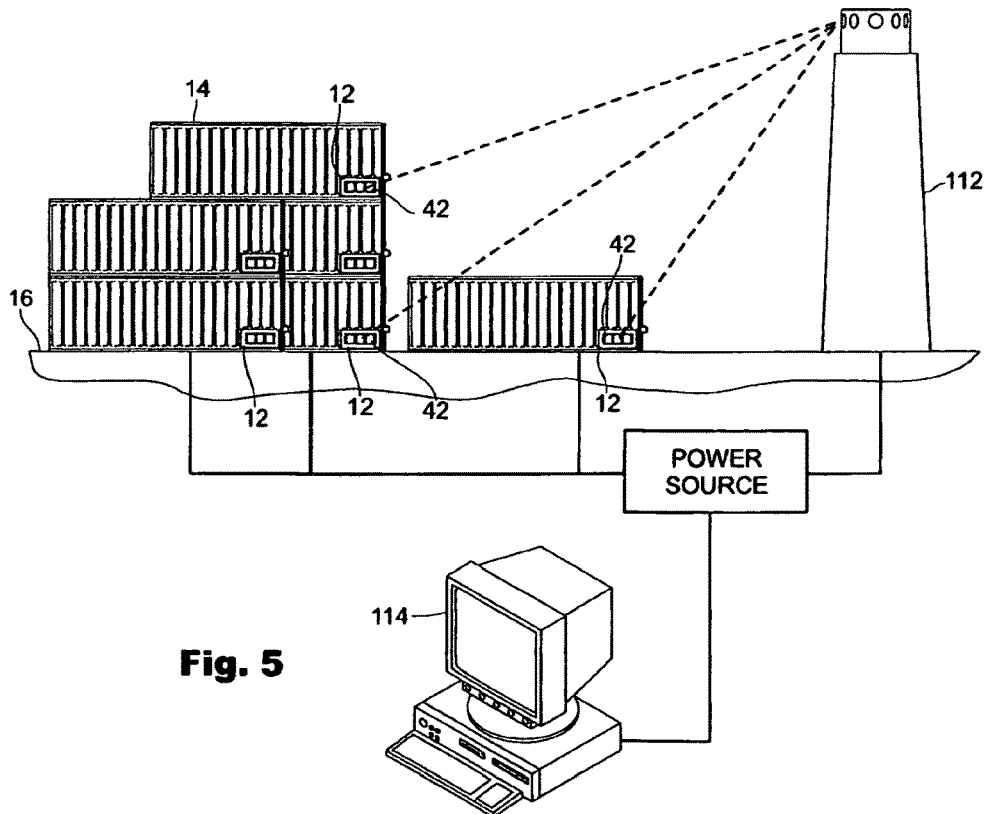
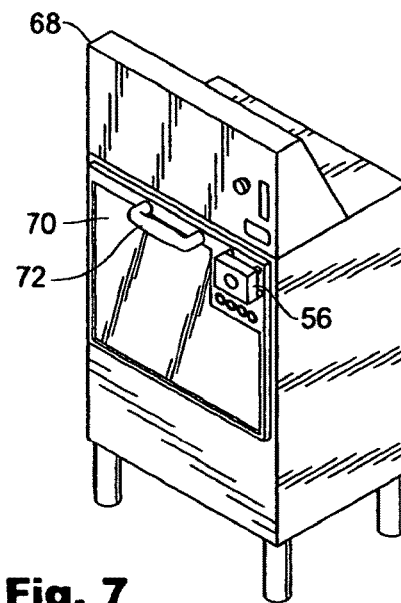
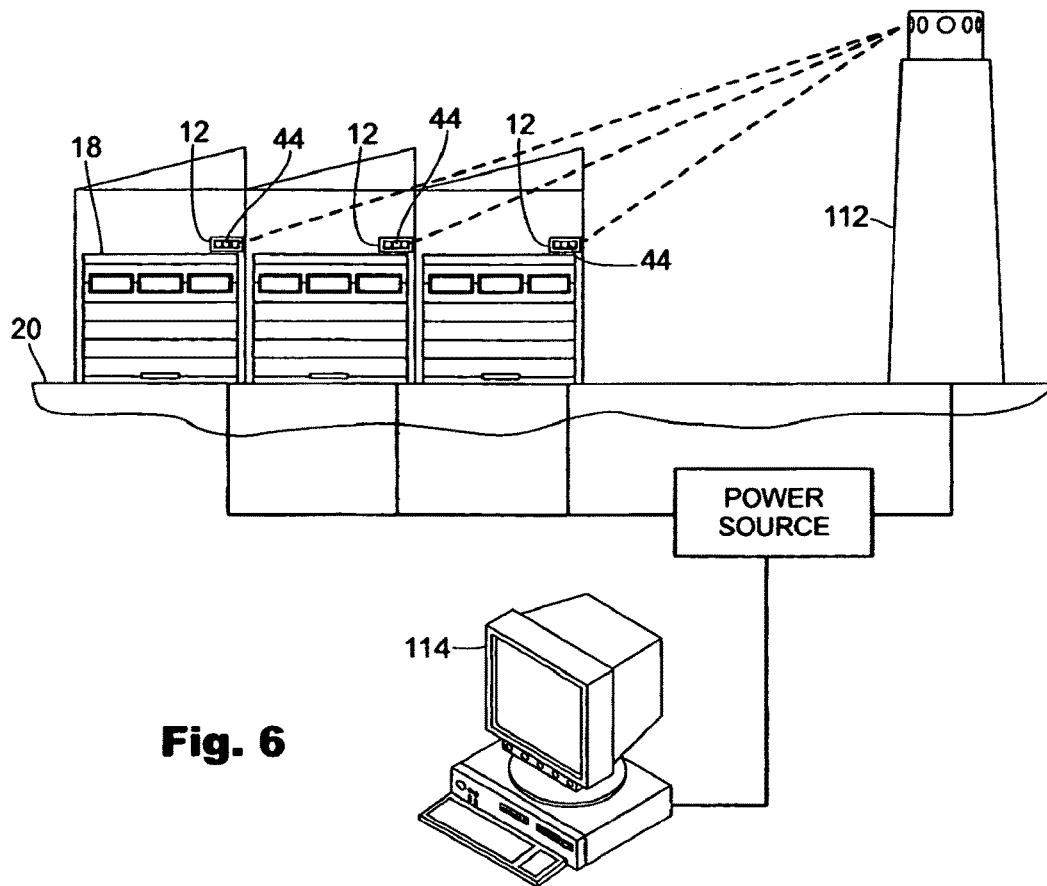


Fig. 5



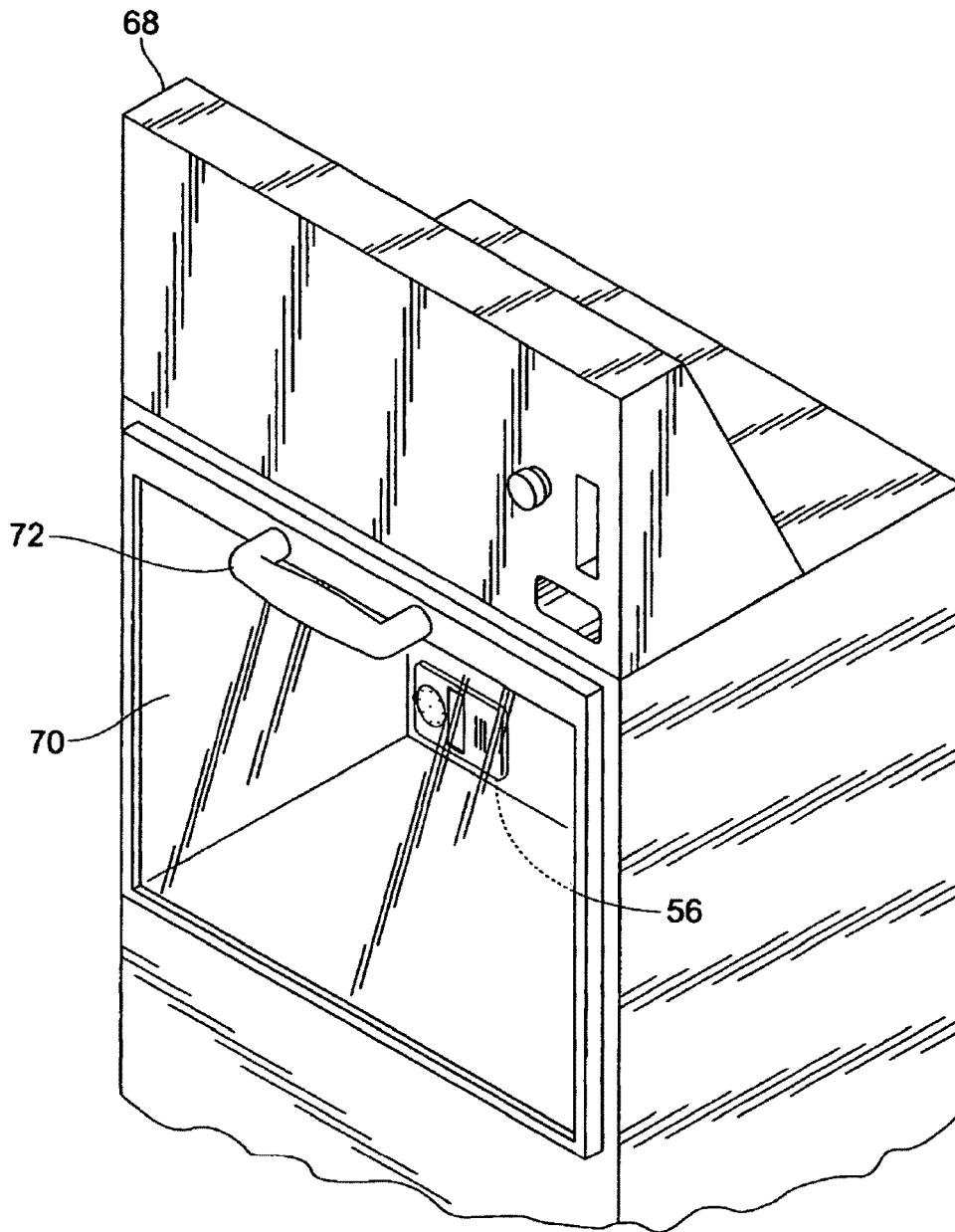


Fig. 8

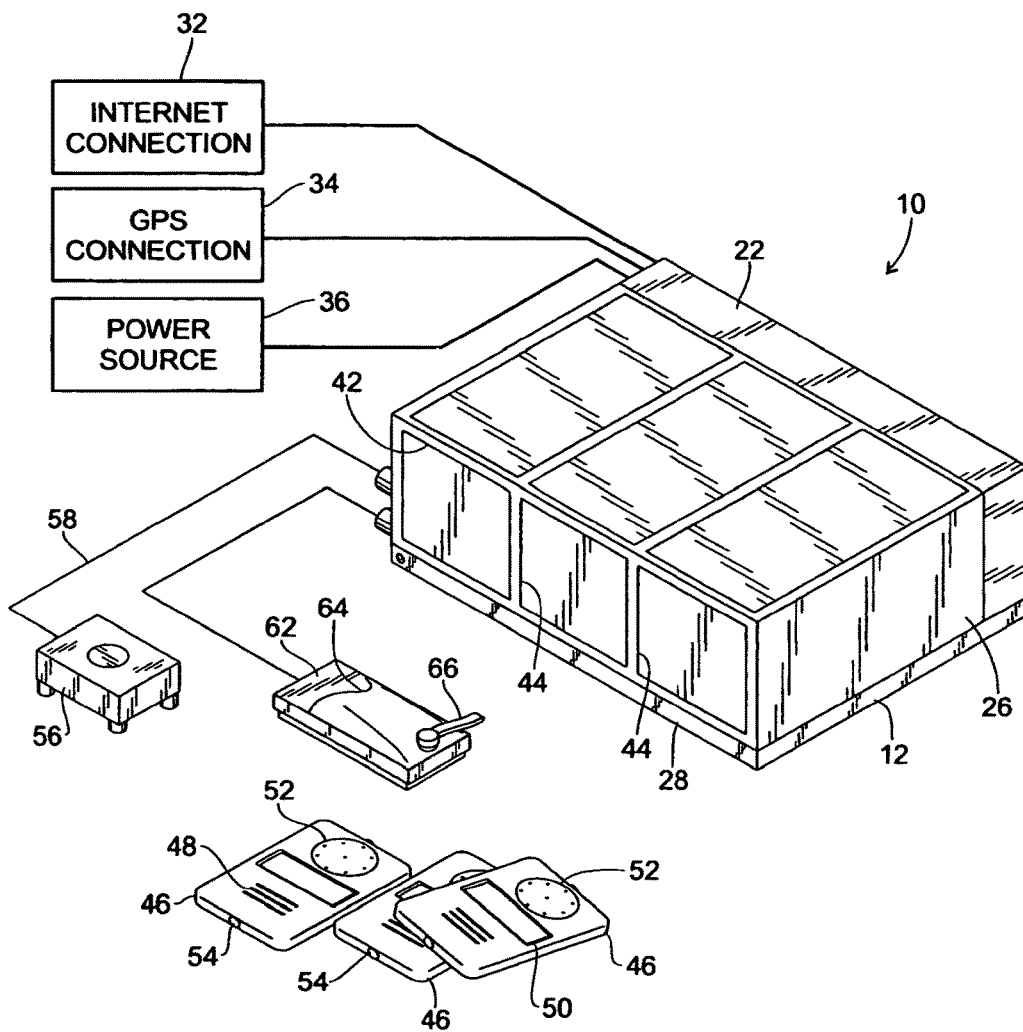


Fig. 9

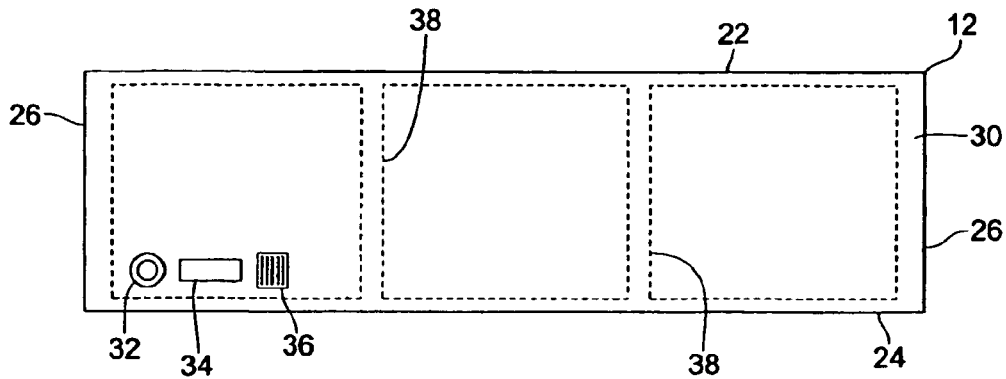


Fig. 10

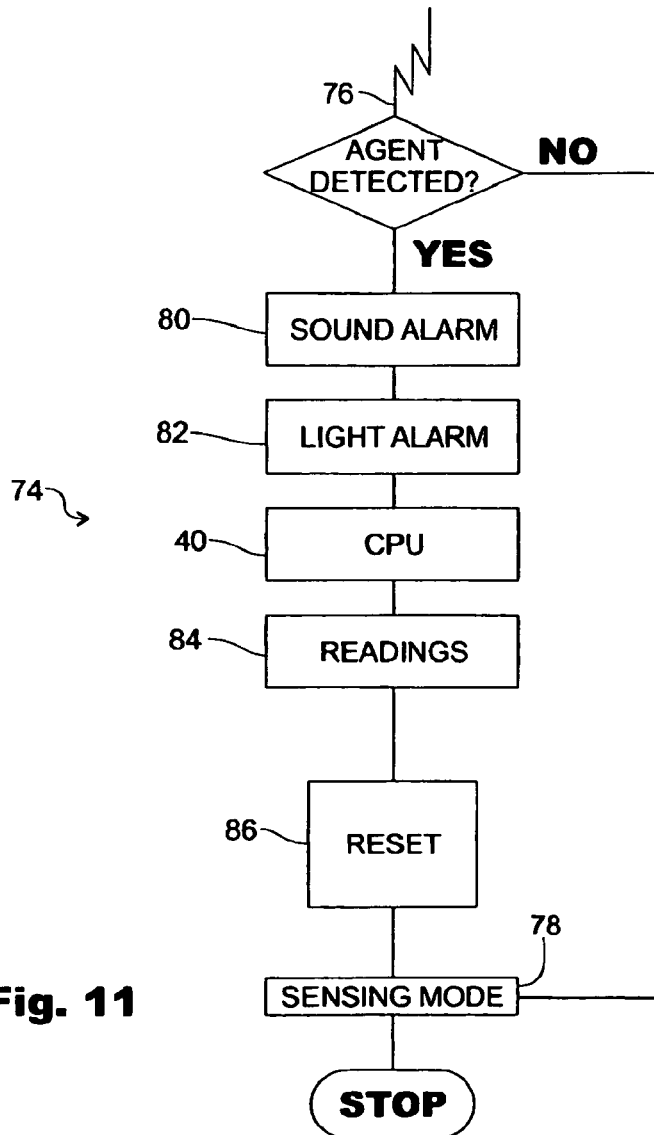


Fig. 11

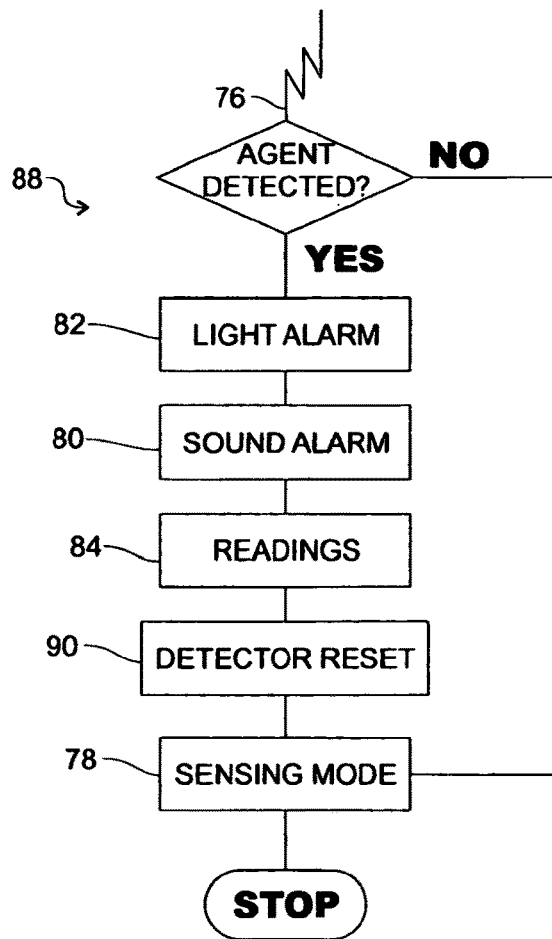


Fig. 12

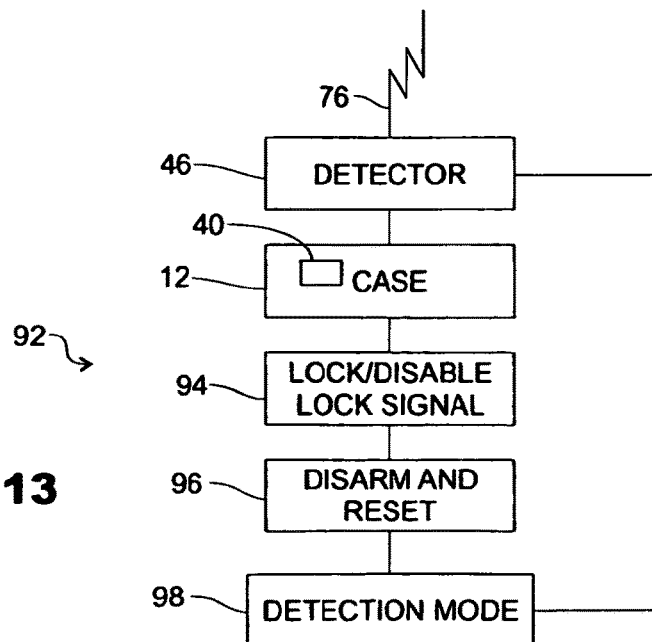
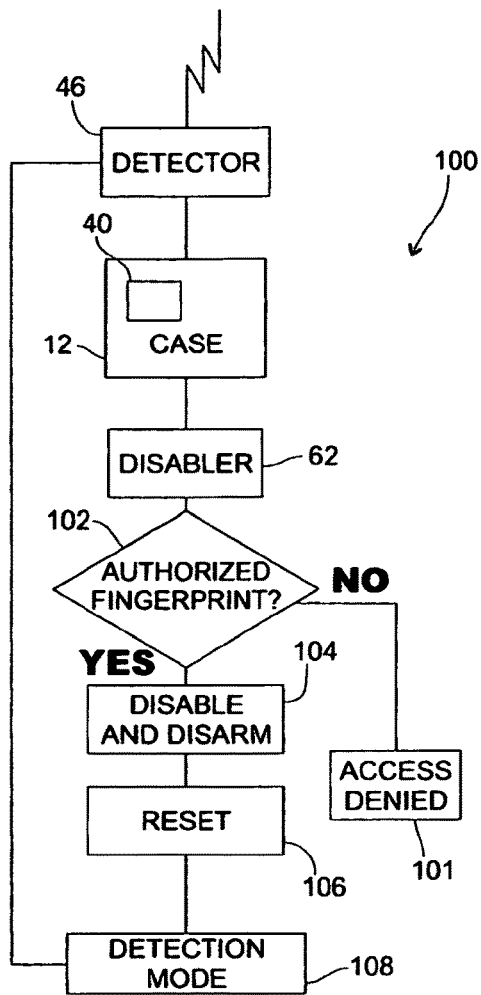
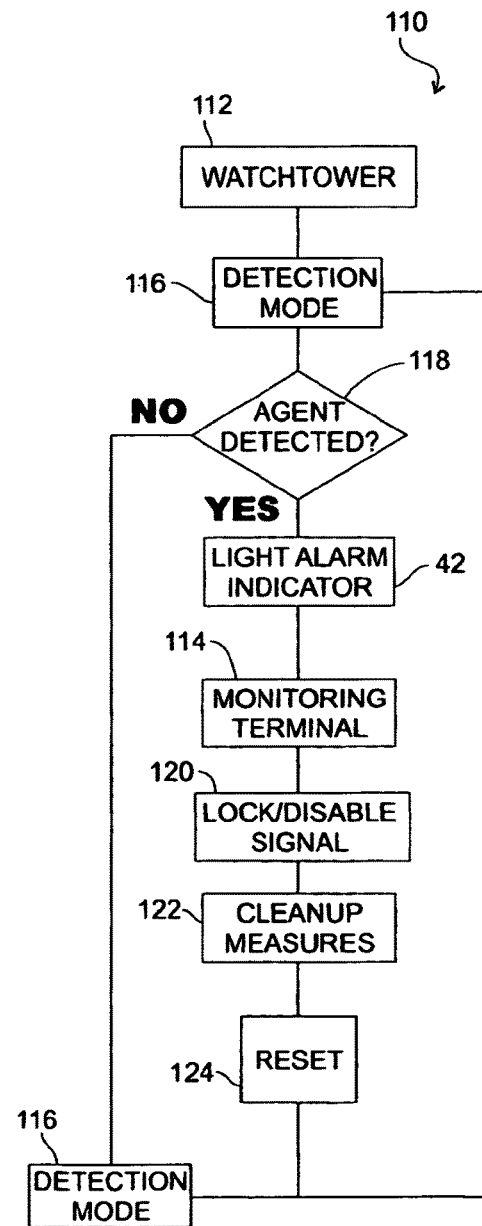


Fig. 13

**Fig. 14****Fig. 15**

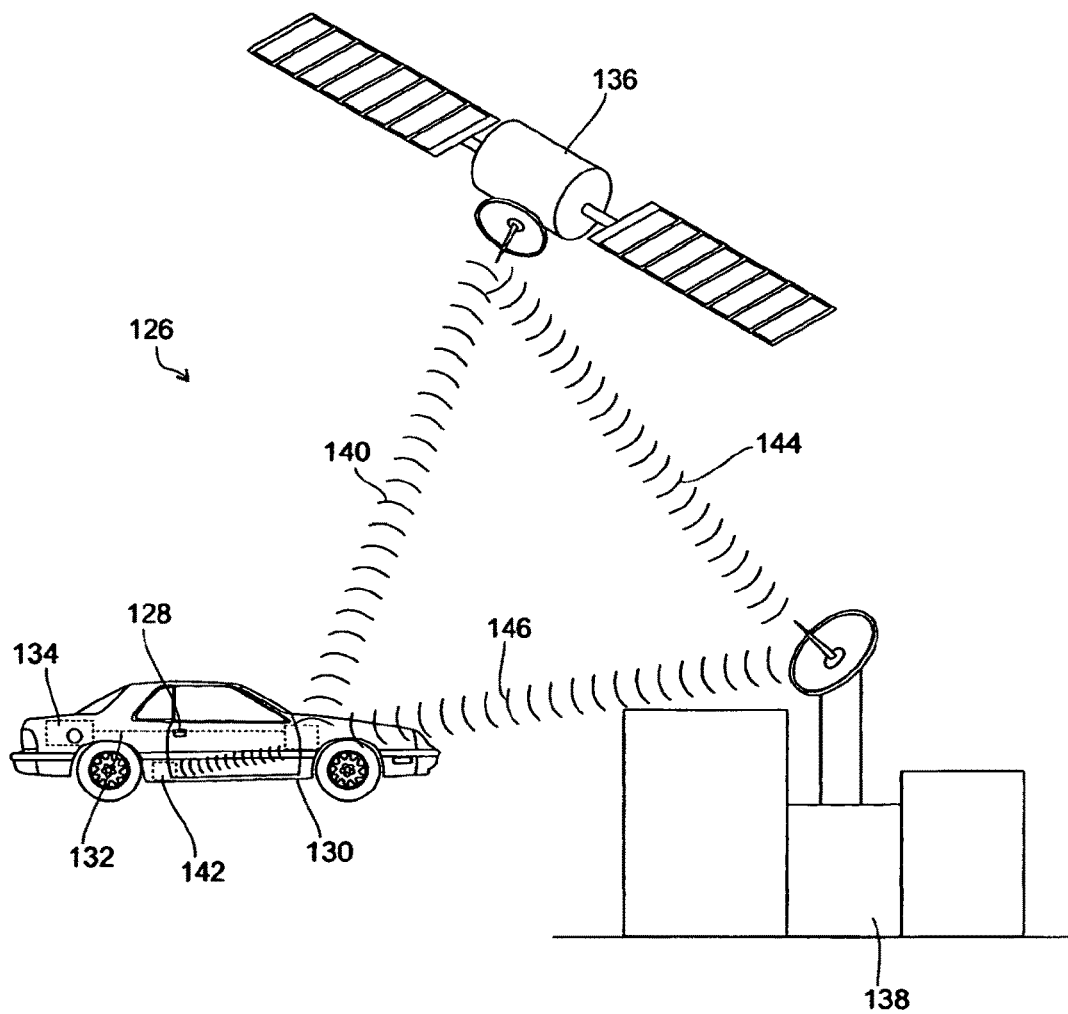
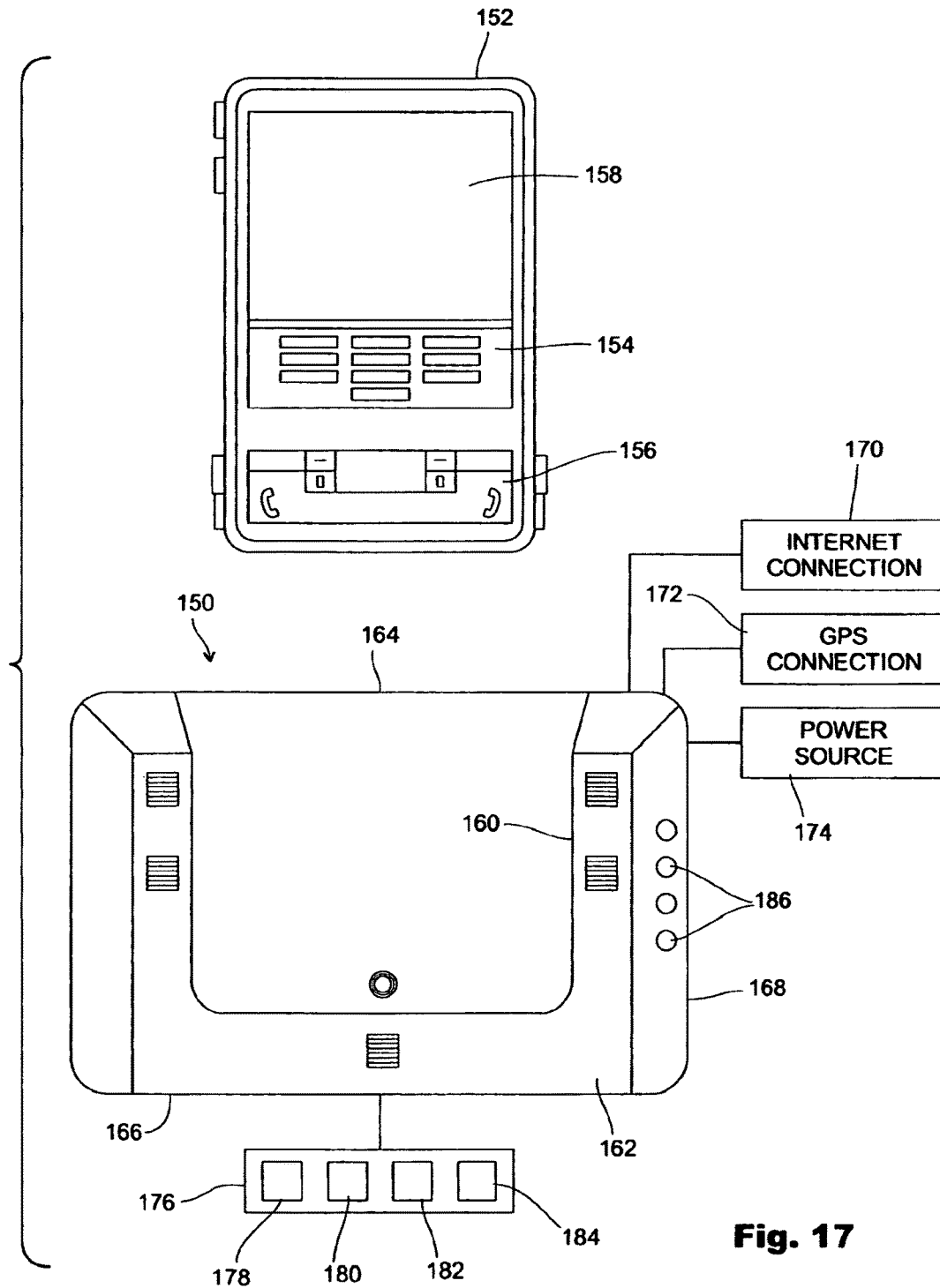


Fig. 16



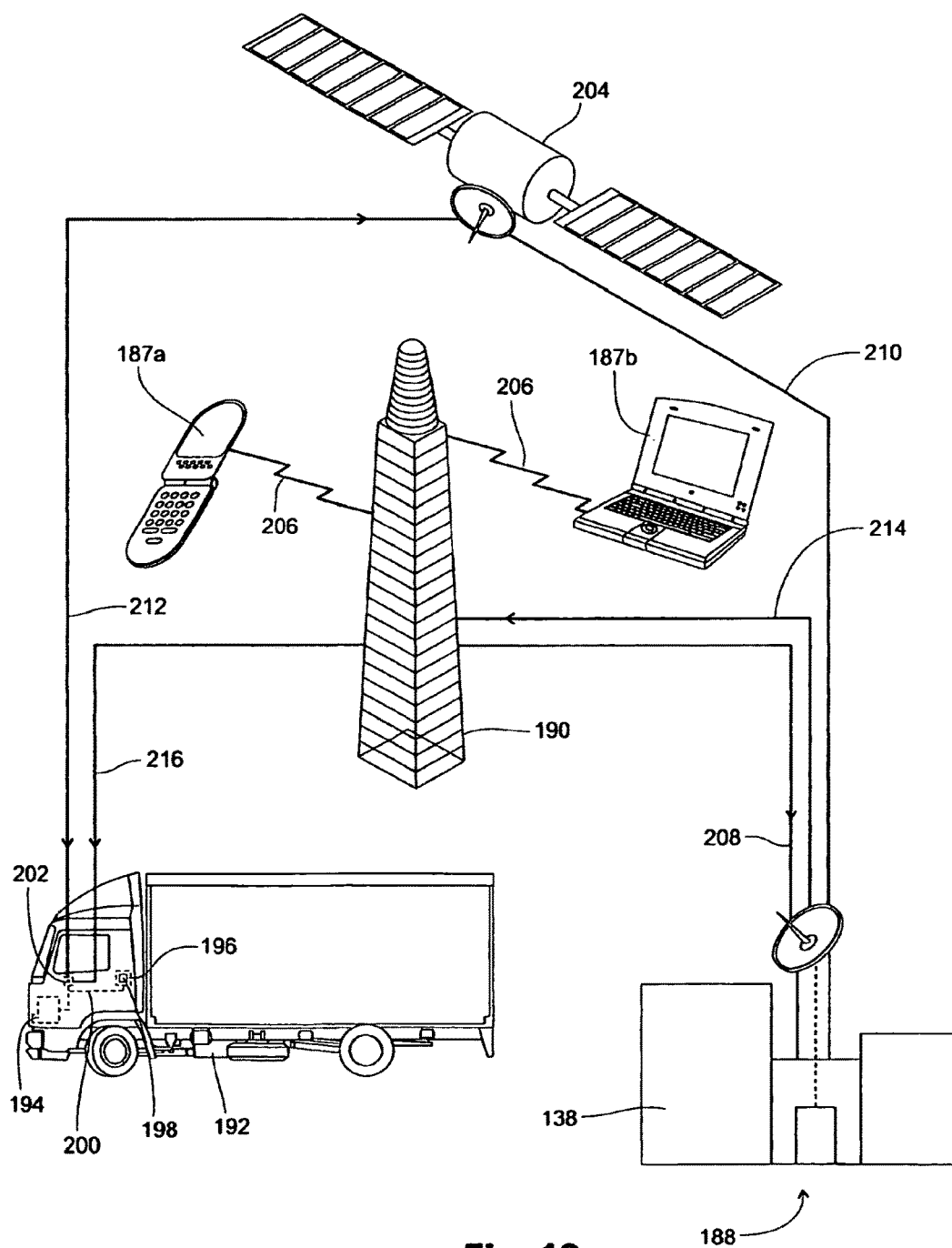
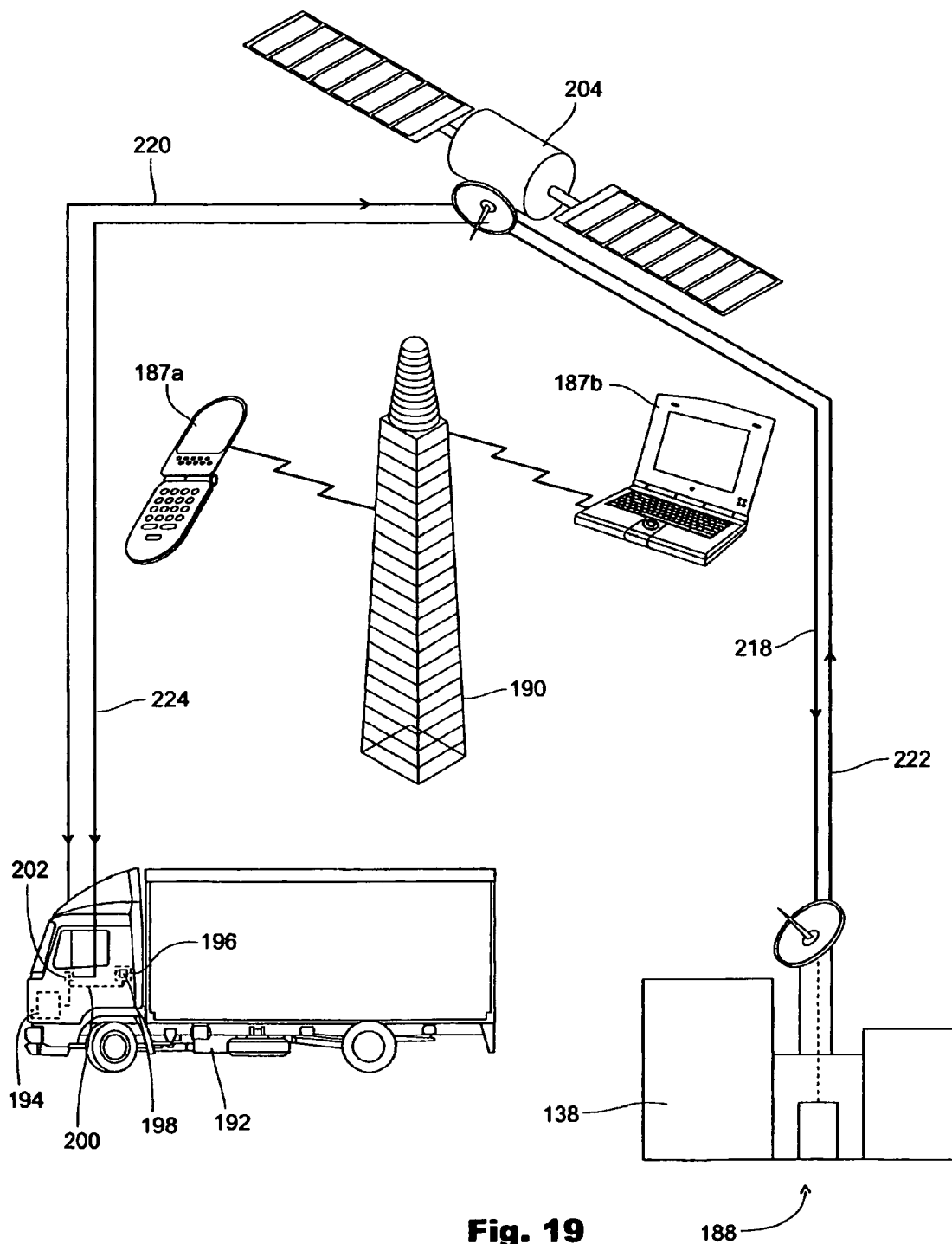


Fig. 18



US 9,589,439 B2

1

MULTI SENSOR DETECTION, STALL TO STOP AND LOCK DISABLING SYSTEM

This application is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 14/021,693 titled "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Sep. 9, 2013 that issued on Aug. 4, 2015 as U.S. Pat. No. 9,096,189, the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. Pat. No. 9,096,189 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 13/288,065 titled "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Nov. 3, 2011 and that issued on Sep. 10, 2013 as U.S. Pat. No. 8,531,280, the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. patent application Ser. No. 13/288,065 that will issue as U.S. Pat. No. 8,531,280 is a divisional application and claims the filing date and benefit of U.S. patent application Ser. No. 12/802,001 titled "Multi Sensor Detection, Stall to Stop, and Lock Disabling System" filed on May 27, 2010, now U.S. Pat. No. 8,334,761, the entire contents and complete subject matter of which are incorporated by reference herein in their entirety for all purposes. U.S. patent application Ser. No. 12/802,001 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 12/657,356 titled "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Jan. 20, 2010, now U.S. Pat. No. 8,106,752 and incorporates the entire contents and complete subject matter therein by reference in their entirety for all purposes. U.S. Pat. No. 8,106,752 is a continuation of and claims priority to U.S. Pat. No. 7,636,033. U.S. Pat. No. 7,636,033 is a continuation-in-part of and claims priority to U.S. Pat. No. 7,385,497. U.S. patent application Ser. No. 13/288,065 that issued as U.S. Pat. No. 8,531,280 also claims the filing date and benefit of and incorporates the entire contents of U.S. patent application Ser. No. 12/657,356, now U.S. Pat. No. 8,106,752 herein by reference for all purposes. The present application also claims the filing date and benefit of and incorporates the entire contents of U.S. Pat. Nos. 8,531,280; 8,334,761; 8,106,752; 7,636,033; and 7,385,497 by reference herein in their entirety for all purposes.

FIELD OF THE INVENTION

The present invention pertains to anti-terrorist detection and prevention systems, and more particularly pertains to a disabling lock mechanism combined with a chemical/biological/radiological detection system for use with products grouped together by similar characteristics in order to prevent unauthorized entry, contamination and terrorist activity.

BACKGROUND OF THE INVENTION

Terrorist activity is a continuous, daily, worldwide threat to the stability, prosperity, security and peace within nations and between and among nations. Its danger lies in its arbitrary destructiveness as much as in its unpredictability, and the constant threat of terrorist activity compels measures and actions that cause strain and contention in free, democratic societies as security concerns and civil liberty concerns must be balanced so that both public safety and civil liberties are maintained. Safety and security concerns can be addressed through numerous proactive steps and measures, many of which cause only minimal interference with and disruption of the daily routines of work, travel, commerce

2

and entertainment. However, because modern industrial societies afford almost limitless places, locations, and opportunities for terrorist activities, no safety measure or security protocol will be foolproof, but many security measures, systems and protocols can be implemented that greatly minimize specific threats through fingerprint identification procedures, chemical, biological, and radiological hazard detections, bomb and explosive detection, and controlling the access to everything from shipping containers to school lockers. Thus, the prior art discloses a wide range of security measures and systems.

For example, the Fishbine et al. patent (U.S. Pat. No. 4,792,226) discloses an optical fingerprinting system that includes an optics/processor unit, a video monitor, a data terminal, and a printer for collecting and storing data characteristics of all ten individual fingerprints for printing demographic information and fingerprint images as desired on a standard booking or applicant card.

The Schiller patent (U.S. Pat. No. 4,544,267) discloses a finger identification unit that includes a fingerprint scanning apparatus using a collimated beam of light to interrogate the fingerprint of a finger placed against a platen so that successive scan positions produce signals containing fingerprint information.

The Fishbine et al. patent (U.S. Pat. No. 5,222,152) discloses a portable fingerprint scanning apparatus for optically scanning and recording fingerprint images and wirelessly transmitting such images to a mobile processing unit for verification and background checking.

The Loughheed et al. patent (U.S. Pat. No. 5,233,404) discloses an optical scanning apparatus that uses a linear charge coupled device (CCD) for recording the image of a fingerprint on the viewing surface.

The Groger et al. patent (U.S. Pat. No. 5,766,956) discloses a diode laser based sensor for undertaking optical, chemical, immunological or nucleic acid-based assay or other chemical analysis.

The Feldman patent (U.S. Pat. No. 5,938,706) discloses a multi element security system for preventing the unauthorized use of an automotive vehicle, and which includes numerous locking and control features interconnected to an onboard cpu.

The Bowker et al. patent (U.S. Pat. No. 5,963,657) discloses a safety access control for doors, handles, locks, etc., wherein the surface relief of a finger is read and verified to either allow or prevent access by the individual to the door, handle, lock, etc.

The Bonder et al. patent (U.S. Pat. No. 6,078,265) discloses a fingerprint identification security system wherein a key lock operated security system utilizes the fingerprint of the individual to control user access to the security system, such as the ignition system of an automotive vehicle.

The Anzai et al. patent (U.S. Pat. No. 6,271,745 B1) discloses a keyless authorization system for use of a motor vehicle that includes fingerprint reading units located on the exterior or interior of the motor vehicle and which is coupled to a control unit for scanning, comparing and matching fingerprints to allow or disallow access to the motor vehicle.

The Hwang patent (U.S. Pat. No. 6,374,652 B1) discloses a fingerprint-activated doorknob in which a detecting sensor for a fingerprint is placed on the doorknob for measuring and searching the fingerprint against previously stored fingerprint inputs to control access to the door.

The Vor Keller et al. patent (U.S. Pat. No. 6,588,635 B2) discloses a safety holster for a firearm that includes a pivotally mounted retaining member and a fingerprint sensor

US 9,589,439 B2

3

for scanning fingerprint information so that only authorized users can withdraw the firearm from the holster.

The Cordery et al. patent (U.S. Pat. No. 6,613,571 B2) discloses a method and system for detecting biological and chemical hazards in the mail that includes sensors placed within the mail box for sampling and testing ambient air and so that mail can be safely transported through the mail system.

The Nagata patent (U.S. Pat. No. 6,628,213 B2) discloses a coding method for digital signal coding and decoding that includes a CMI (code-marked inversion) method of signal coding.

Nonetheless, despite the ingenuity of the above devices, methods, and systems, there remains a need for a multi-detector and disabling lock system for use with various types of products collected together by common characteristics into product groupings for detecting chemical, biological and radiological agents and compounds and for selectively disabling and activating the product locks thereby preventing unauthorized entry and further contamination and preventing and thwarting terrorist activities.

SUMMARY OF THE INVENTION

The present invention comprehends a chemical/biological/radiological detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping 1 include, but are not limited to, cargo containers, shipping containers, tractor trailers, snail carriers, mail boxes and lockers; while the products grouped into what may be referred to as Product grouping 2 include, but are not limited to, chemical, biological, radiological, and nuclear detectors, motion sensors and door sensors. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

The multi sensor detection and lock disabling system includes a detector case sized to fit in, upon or adjacent any of the aforescribed products for detecting harmful and dangerous chemical, biological, and radiological agents, compounds and elements. In addition, the multi sensor detection and lock disabling system is capable of transmitting a signal to lock or disable a lock on the product, and is also capable of transmitting signals to a monitoring computer terminal or PC so that appropriate defensive and safeguarding actions can be undertaken and an authorized individual can disarm and reset the locking system and the multi sensor detection system. The detector case includes a power source (battery or electrical), interior compartments, Internet and GPS connections and a cpu interconnected with the Internet and GPS connections, and also interconnected with one or more off site monitoring computer terminals or PCs. The detector case includes one or more light alarm indicators that are externally visible and that light up when the chemical, biological, or radiological agent or compound is detected, and the light alarm indicators (which can be indicator lights or panels on the front of the detector case) can be color coded for denoting the specific agent or

4

compound detected, i.e., separate and distinct colors for indicating detection of the chemical, biological, or radiological agent or compound.

The detector case is designed to hold within the interior compartments one or more interchangeable detectors, and each detector is adapted and set up to sample a specific compound or agent. Each detector includes a sound alarm, a sensor, a light alarm, and a readings panel, and is electrically interconnected (either by wire or wirelessly) to the cpu of the detector case so that information regarding the detection of the particular agent or compound can be conveyed from the detectors to the detector case cpu. Each detector can also be used as a manual, stand-alone hand held scanner.

The multi sensor detection and lock disabling system can be interconnected to a surveillance watchtower, as well as monitoring computer terminals or PCs, with the watchtower scanning shipping and cargo crates and containers being prepared for shipment or sitting for extended periods of time on a dock or at a port, at a railway site, or at an industrial storage facility. The watchtower will scan the cargo and shipping crates and containers for the light alarm indicators on detector cases that are mounted in or upon the crates and containers, and thus continuous security surveillance of the crates and containers can be maintained.

An enhanced version of the multi sensor detection and lock disabling system can be employed to prevent car and vehicle bombings. Coupling the multi sensor detection and lock disabling system with satellite service will enable the detection system to detect explosives and transmit an alert signal by satellite to monitoring equipment at a monitoring site. Upon receiving the alert signal at the monitoring site the monitoring equipment activates a stall-to-stop process for disabling the air, fuel, electrical and/or computer system of the vehicle. Moreover, upon receiving the alert signal at the monitoring site the car or vehicle will be locked by transmission of a satellite signal that disables the vehicle's electrical and ignition system thereby preventing escape of the terrorist.

It is an objective of the present invention to provide a multi sensor detection and disabling lock system for securing news racks and vending machines in order to prevent theft, unauthorized use and terrorist activity.

It is another objective of the present invention to provide a multi sensor detection and disabling lock system for preventing terrorist activity by using products grouped together by common features in several product groupings such as design similarity, similarity in the presentation of security problems and similarity with regard to the presentation of solutions to preventing terrorist solutions.

It is still yet another objective of the present invention to provide a multi sensor detection and disabling lock system that is capable of disabling an existing lock or activating a lock inside any of the products of the product grouping lists when a detector or sensor of the system is activated.

It is still yet a further objective of the present invention to provide a multi sensor detection and disabling lock system wherein the disabling lock system prevents the unauthorized entry, access and further contamination of the products included in the several product groupings.

A still further objective of the present invention is to provide a multi sensor detection and lock disabling system that utilizes a multi-task device for preventing terrorist activity to vulnerable products that are collected or arranged by product grouping categories.

Yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system

US 9,589,439 B2

5

to secure cargos and containers, especially cargo and shipping containers, against chemical, biological, radiological and nuclear terrorist activity.

Still another objective of the present invention is to provide a multi sensor detection and disabling lock system capable of detecting chemical, biological and radiological agents and compounds.

Still yet another objective of the present invention is to provide a multi sensor detection and disabling lock system that includes interchangeable detectors that operate in conjunction to detect chemical, biological and radiological agents and compounds.

Still yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system that can be implemented by business or government at a minimum cost by organizing the products to be protected into product grouping categories.

Another objective of the present invention is to provide a multi sensor detection and disabling lock system that accurately and reliably detects harmful agents, compounds and elements, and prevents the placement and storage of weapons and bombs in the range of storage containers and facilities currently available.

Still, another objective of the present invention is to provide a multi sensor detection and disabling lock system wherein the interchangeable detectors that comprise part of the system can be used as stand-alone scanners.

These and other objects, features, and advantages will become apparent to those skilled in the art upon a perusal of the following detailed description read in conjunction with the accompanying drawing figures and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the primary features of the system which include a detector case, several interchangeable detectors, an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler;

FIG. 2 is a front elevation view of the multi sensor detection and lock disabling system of the present invention illustrating one of the interchangeable detectors first shown in FIG. 1;

FIG. 3a is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one lock disabler to the lock of a product, such as a container, and disengaged from the lock of the container;

FIG. 3b is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the engagement of the lock disabler to the lock of the product for locking or disabling the lock of the product so that unauthorized access is prevented;

FIG. 4 is a side elevation view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case mounted to the product, such as the container, with the light alarm indicators externally visible;

FIG. 5 is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of detector cases with a surveillance watchtower and a monitoring PC terminal;

FIG. 6 is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the placement of detector cases upon containers different

6

from the containers of FIG. 5, and wherein the detectors case are interconnected to a surveillance watchtower and a monitoring PC terminal;

FIG. 7 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one automatic/mechanical lock disabler to the lock of a standalone news rack;

FIG. 8 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating one interchangeable detector placed within the standalone news rack;

FIG. 9 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case having color coded front panels for specifically indicating the agents, compounds or elements that have been detected;

FIG. 10 is a rear elevation view of the multi sensor detection and lock disabling system of the present invention illustrating the GPS, Internet and power source connections;

FIG. 11 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector with the detector case and the steps undertaken by the system when an agent or compound is detected;

FIG. 12 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the sequence of steps undertaken by one detector when functioning as a standalone scanner for detecting an agent or compound;

FIG. 13 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector case with the automatic/mechanical lock disabler for activating the lock disabler upon detection by the system of an agent or compound;

FIG. 14 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating interconnection of the detector case with the fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public upon detection of the agent or compound;

FIG. 15 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the system with a surveillance watchtower and a monitoring PC or computer terminal for monitoring containers, such as shipping or cargo containers, that may sit for extended time periods on docks, at rail yards, and at industrial storage facilities;

FIG. 16 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the integration of the detection system with a satellite and monitoring equipment at a monitoring site for detecting explosives placed in a vehicle and then transmitting signals to the satellite and then to the monitoring site for disabling and locking the vehicle;

FIG. 17 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the features and elements of the detector case to a cell phone and cell phone case;

FIG. 18 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of a OPS satellite, a monitoring site and a cell phone tower for communicating to and with an electronic device such as a laptop computer or a cell phone

US 9,589,439 B2

7

for transmitting signals to a vehicle for activating an onboard stall-to-stop device for bringing the vehicle to a halt; and

FIG. 19 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the use of a GPS satellite in conjunction with the monitoring site and monitoring equipment to relay commands and signals to the cpu or transceiver of the vehicle for stopping or locking the vehicle in response to a signal that a certain type of event (detection of a bomb, engine failure or malfunction or unauthorized use) has occurred or is in process

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Illustrated in FIGS. 1-19 is a multi sensor detection and lock disabling system 10 for preventing terrorist activity by monitoring, detecting, and securing those critical areas, sites, and facilities vulnerable to terrorist activity. The first step is the identification of critical areas, sites, locations and facilities that are vulnerable to terrorist activity as convenient places to store and plant explosives and bombs and spread biological, chemical or radiological agents and compounds, followed by the disposition of the multi sensor detection and lock disabling system 10 for monitoring, detecting, and securing the particular location or site. Vulnerable sites, locations, facilities and areas are nearly limitless in their variety; in order to categorize the protection the present invention provides an anti-terrorist product grouping strategy has been developed wherein products made from the same or similar material, products having the same or similar design, and products presenting the same or similar security problems are grouped together with the multi sensor detection and lock disabling system 10 for preventing terrorist activity. For example, two preferred product groupings can be Product Grouping I: cargo containers, shipping containers, cargo planes, freight train cars, tractor trailers, mail carriers (UPS, FedEx), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans and utility vehicles. Product Grouping II: chemical detectors, biological detectors, radiological detectors, nuclear detectors, motion sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems. In addition to grouping products together by features, designs and materials, the multi sensor detection system 10 includes a lock disabling capability for disabling an existing lock or activating a lock on or inside any of the aforementioned products when a detector or sensor of the system is activated. The lock disabling feature is a crucial component of the invention in so far as it prevents unauthorized, unequipped or untrained individuals from gaining access and entry to the site and causing further contamination of the site.

As shown in FIGS. 1-10, the multi sensor detection and lock disabling system 10 includes at least one—and preferably many—detector case 12 that can be placed in, on, upon or adjacent the product, such as the shipping containers 14 of FIGS. 4 and 5 resting upon a platform 16 or the cargo container 18 of FIG. 6 sitting upon a seaport dock or pier 20. The detector case 12 includes a top 22, a bottom 24, a pair of opposed sides 26 and a front side or panel 28 and an opposite rear or back side 30. The rear side 30 has connections or contacts that can include an Internet connection 32,

8

a GPS connection 34 and a power connection 36 for a power source. The power source for the detector system 10 can be any conventional battery or electrical source. The detector case 12 includes an interior chamber divided into a number of compartments 38 for holding therein agent or compound detection means hereinafter further described. A cpu 40 is mounted within the detector case 12 and electrically interconnects, routes, and transmits signals among items hereinafter further described and also communicates with a monitoring site and monitoring equipment. The front side 28 of the detector case 12 includes indicator means for visually indicating that a specific agent, compound or element has been detected. The indicator means can include color coded indicator lights 42 in panel form, as shown in FIG. 9, with each indicator light panel 42 lighting up with a specific color corresponding to the detection of a specific agent or compound; or color coded indicator lights 44, as shown FIG. 1, that correspond to and individually light up on the detection of a specific agent or compound (chemical, biological, or radiological).

As shown in FIGS. 1, 2 and 9-13, the multi sensor detection and lock disabling system 10 includes a plurality of detectors 46 with each detector 46 adapted for and set up to sample for a specific agent or compound (biological, chemical, or radiological); and the detectors 46 are interchangeable for adapting to the needs and demands of future technology. The detectors 46 can also be used as standalone scanners. In the preferred embodiment of the invention, at least three detectors 46 are placed within the detector case 12 with one detector 46 for specifically sampling biological agents or compounds, one detector 46 for sampling chemical agents or compounds, and one detector 46 for sampling radiological agents or compounds. The detectors 46 are interconnected to the cpu 40 of the detection system 10 by conventional connections that can be wire or wireless for transmitting the appropriate signals to the cpu 40 upon detection of the particular agent or compound. As shown in FIG. 2, each detector 46 includes on its front plate or facing surface a sound alarm indicator 48, a readings panel 50 comprising a plastic shield and LED lights for displaying the various read-out messages, a sensor 52 for detecting the specific agent, element or compound, and a light alarm indicator 54 that can be color coded for each specific agent and which is externally visible when the detector 46 is used as a stand alone scanner. Each detector 46 includes a conventional microprocessor for controlling the various functions and generating the appropriate signals for transmission to the cpu 40 of the detector case 12.

As shown in FIGS. 1, 3a, 3b, 9, and 13-15, used in conjunction with the multi sensor detection and lock disabling system 10 is at least one automatic/mechanical lock disabler 56—and depending upon the number of products being monitored there can be one lock disabler 56 for each product. The automatic/mechanical lock disabler 56 is physically connected to the detector case 12 by a wire or cable 58 for receiving signals therefrom for disabling an existing lock or activating a lock inside a product to prevent access to the product. By way of example, FIG. 3a shows the automatic/mechanical lock disabler 56 mounted—by any conventional means—to the lock 60 of the shipping container 14 shown in FIGS. 4 and 5 and connected by wire 58 to the cpu 40 of the detector case 12. The lock disabler 56 is in the non-activated or disengaged state in FIG. 3a. FIG. 3b shows the automatic/mechanical lock disabler 56 mounted to the lock 60 of the shipping container 14 and in the activated or engaged state after detection of an agent or compound by the system 10 thereby for locking or disabling

US 9,589,439 B2

9

the lock 60 of the shipping container 14 and preventing unauthorized entry and access by unauthorized, untrained and unequipped individuals. In FIGS. 3a and 3b the lock 60 secures doors of the shipping container 14 that can be slidably or pivotably opened and closed.

In addition to the automatic/mechanical lock disabler 56, the multi sensor detection and lock disabling system 10 can also utilize a fingerprint biometric lock with disabler 62 as shown in FIGS. 1 and 14. The fingerprint biometric lock with disabler 62 is interconnected to the cpu 40 of the detector case 12 for receiving transmissions therefrom after detection of an agent or compound has occurred so that the lock on the product can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler 62 occurs when the fingerprint of the individual is placed on the fingerprint-matching pad 64, and if a match occurs with a known fingerprint stored by the cpu 40, then the individual can reset the fingerprint biometric lock with disabler 56 by turning the manual lock disabler 66. The fingerprint biometric lock with disabler 62 is mounted to the lock of the product in a manner similar to the mounting of the automatic/mechanical lock disabler 56 that is shown in FIGS. 3 and 3b.

FIGS. 4 and 5 show one manner of disposition or placement of the detector case 12 in relation to the product, i.e., the shipping container 14, with the color coded indicator lights 42 externally viewable; FIG. 5 shows a number of shipping containers 14 each equipped with a detector case 12 and integrated with elements hereinafter further described for continuously monitoring the shipping containers 14 as they sit for an extended period of time on the truck or rail platform 16. FIG. 6 illustrates several cargo containers 18 sitting on the shipping dock or pier 20, with each cargo container 18 having a detector case 12 mounted thereon and integrated with and monitored by elements shown in FIG. 5 and hereinafter further described.

FIG. 7 illustrates a typical product from product grouping 1 that is monitored by the multi sensor detection and lock disabling system 10 of the present invention; specifically, FIG. 7 shows a news rack 68 with one automatic/mechanical lock disabler 56 mounted to and interconnected with the locking mechanism of the news rack 68. As long as there is no detection of any agent or compound, the lock disabler 56 is in the disengaged state, and the individual can deposit the coin amount in the chute and then freely open the glass panel 70 by the handle 72 for removing a paper. However, the lock disabler 56 would be activated upon detection of the harmful agent or compound and receipt of a signal from the cpu 40 for locking or disabling the locking mechanism thereby denying access to the interior of the news rack 68 from all untrained, unauthorized and unequipped individuals.

FIG. 8 illustrates one detector 46 disposed within the news rack 68 and which is visible through the panel 70 for detecting one specific agent, compound or element. The detector 46 functions as a stand-alone scanner and can be wirelessly interconnected to offsite monitoring equipment.

FIG. 11 illustrates a representative schematic 74 for describing the signal transmission process from the detector 46 to the cpu 40 of the detector case 12. The external stimulus 76 would be the chemical, biological or radiological agent or compound. If there is no detection of the agent or compound, the detector 46 will stay in the sensing mode 78. However, detection of the specific agent will trigger the sound alarm 80 and the light alarm 82, and instant transmittal of a signal to the cpu 40. The readings 84 can be stored by the cpu 40 for verification and future review and evaluation. After all the appropriate corrective and preventative

10

measures have been undertaken by the trained and authorized personal, and the site has been cleansed of the contamination, authorized and equipped personal can then reset 86 the system 10.

FIG. 12 illustrates a representative schematic 88 for the detector 46 when used as stand-alone scanner. The detector 46 undergoes the same essential steps as illustrated in FIG. 11, with the exception of the signal transmission to the cpu 40. The detector 46 remains in detection mode 78 until an agent is detected, and then the various functions—light alarm 82, sound alarm 80, storage of readings 84, and, after the appropriate security and safety steps have been carried out by authorized personal, detector reset 90 by authorized personal can occur thereby placing the detector 46 back in detection or sensing mode 78.

FIG. 13 is a representative schematic 92 that illustrates the steps undertaken by the system 10 to lock or disable a lock, such as the lock 60 for the shipping container 14 shown in FIGS. 3a and 3b. Upon detection of the agent (chemical, biological, radiological) the alarm light indicators 42 or 44 will light up providing external indication that an agent has been detected. In addition, the system 10—the cpu 40—will transmit a lock/disable lock signal 94 to the automatic/mechanical lock disabler 56 to lock or disable the lock on the product, such as the lock 60 on the shipping container 14 of FIGS. 3a-5. This prevents unauthorized, unequipped, or untrained individuals from entering or gaining access to the product for which a dangerous and perhaps lethal agent has been detected. After the proper authorities and authorized personal have been notified and all the appropriate security, preventative and clean up measures have been undertaken, the authorized individual can perform the disarm and reset function 96 for the system 10 placing the system 10 in back in the detection mode 98.

FIG. 14 is a representative schematic 100 illustrating the use of the fingerprint biometric lock with disabler 62 with the system 10. Upon detection of the agent or compound by the detector, the various alarms would sound and light up (shown in previous figures), and the cpu 40 would then transmit a signal to the fingerprint biometric lock, with disabler 62 to lock or disable the lock on the product, such as the lock 60 on the shipping containers 14 shown in FIGS. 3a-5. The shipping containers 60 would remain locked and in an access denied mode 101 should an attempt be made to gain access to the container 60 by opening the lock 60 with an unauthorized fingerprint. However, a fingerprint that matches stored and authorized fingerprints 102 would indicate an authorized individual, and would allow the individual to disable and disarm 104 the lock 60 of the shipping container 14. The fingerprint biometric lock with disabler 62 would then be reset 106 after the appropriate safety, cleanup, and protection measures are completed, and the system 10 would be reset and placed back in the detection mode 108.

FIG. 15 is a schematic representation 110 that illustrates the integration of a surveillance watchtower 112 and a monitoring terminal or PC 114 for monitoring products such as the shipping containers 14 or cargo containers 16 that sit for extended periods of time of docks, piers 20, truck terminals, rail yards, shipping platforms 16 and industrial sites as shown in FIGS. 5 and 6. The watchtower 112 would maintain continuous surveillance over a number of shipping containers 60, for example, with detector cases 12 mounted in or on each container 14 and set in detection mode 116 with one or more detectors 46 disposed in each detector case 12. The watchtower 112 would continuously scan for light alarm indicators 42 and 44 on the products, such as the containers 14 or 18, and the watchtower 112 would be interconnected

US 9,589,439 B2

11

and integrated with the monitoring terminal or PC 114. Upon detection 118 of an agent or compound in one or more of the shipping containers 14, the appropriate light alarm indicators 42 or 44 would provide visible confirmation of the detection of the specific agent or compound. The cpu 40 would transmit a lock/disable signal 120 to the lock 60 on each respective shipping container 14 to lock or disable the lock 60 thus preventing access to that respective shipping container 14. In addition, signal transmissions would be sent to the monitoring terminal or PC 114 (which could be off site) thereby alerting authorized security personnel of the contamination event. With the information received at the monitoring terminal 114, authorized personnel would then be notified and dispatched to the area to undertake the appropriate safety and cleanup measures 122. Such measures would also include disarming the lock disabling system in order to gain access to the shipping container 14. After all the cleanup and security measures are completed by the trained and properly equipped authorities, the detection system and the lock disabling feature would reset 124 and the detection system would again be placed in detection mode 116.

FIG. 16 is a schematic representation 126 that illustrates an enhanced version of the multi sensor detection and lock disabling system 10 for preventing car and vehicle attacks and bombings. The lock disabling system 10 would be interconnected to the locking system and mechanism 128 of the vehicle 130. In addition, a stall to stop disabling link 132 can be made with the fuel, air, and electrical system 134 of the vehicle 130. The enhanced version incorporates a satellite 136 for signal receipt and transmission from the vehicle 130 in which the detector system 10 is placed to a monitoring site and monitoring equipment 138. As shown in FIG. 16, a detection signal 140 would be sent to the satellite 136 by the detection system 10 upon detection of a bomb or explosive 142 hidden in the vehicle 130. The satellite 136 would then transmit an alert signal 144 to the monitoring site 138 with the signal 144 containing the relevant data to evaluate the nature of the threat. The monitoring site 138 would then transmit a stall to stop signal 146 to the detection system 10 to lock the vehicle 130 and/or disable the electrical system of the vehicle 130 thereby disabling the vehicle 130, preventing access to the vehicle 130 by locking the vehicle 130, and preventing any terrorist in the vehicle 130 from escaping.

The detector case 12 can be modified and adapted for inclusion with cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, suitcases, and briefcases. In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring.

The system 10 and the watchtower 112, along with the satellite 136 and the monitoring site 138 can be adapted or incorporated with cell phone towers and satellites for use with satellite communication and/or a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu 40, a transceiver and monitoring equipment to include but not be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween. The aforementioned telecommunication and radio communication means can be interactive with any type of motive vehicle that includes but is not limited to cars, trucks, vans, SUVs, trains, subways, boats, ships and airplanes, and which is reported stolen, experiences a loss of brakes, or a

12

bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted to the vehicle and which detection causes an automatic signal transmission or a signal transmission is activated when a call is made to the monitoring station by an authorized person. The authorized individual includes but is not limited to the owner, pilot, conductor, captain, police highway patrol, security guard and military personnel to the monitoring equipment for activating a vehicle slowdown or stall-to-stop disabling system that similar to the disabling system 126 shown in FIG. 16, or incorporating features of the system 126 shown in FIG. 16, from the monitoring equipment to the vehicle. The activation of the stall-to-stop disabling means or the vehicle slowdown disables or engages the computer, electrical, fuel and air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to the brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.

In addition, the basic stall-to-stop disabling means or the vehicle slowdown means and device can be adapted, modified or designed to include: an open bust or open platform for integrating any new and innovative technology; warning lights indicators; sound alarm indicators; voice alarm indicators; a cell phone to transmit to the vehicle a signal for slowing and halting the vehicle; and a lock disabling system or means to lock a thief or terrorist inside the vehicle after a transmission is received or sent. Open bust or open platform also refers to the compatibility of the detector case 12, or the incorporation of its features in cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, briefcases, and suitcases, etc., with other communication, transmission and surveillance systems whereupon the detector case 12, and its features, can be seamlessly integrated with other new and emerging systems and technologies.

Thus, as shown more specifically in FIG. 17, by way of a representative example the features and elements of the detector case 12 are shown as being incorporated into cell phone detector case 150 and associated cell phone monitor 152. The cell phone monitor 152 includes the standard keypad functions 154 and more specialized system use (ring tone, email, photos, texting) functions 156 as well as a viewing screen 158. The cell phone detector case 150 includes a recharging cradle or seat 160, a front side 162, a top 164, a bottom 166, and a pair of opposed sides 168. At the back of the cell phone detector case 150 are connections, contacts, and ports for at least an Internet connection 170, a GPS connection 172, and a contact, plug, or port for a power source 174. The power source for the cell phone detector case 150 can be any conventional rechargeable battery source or standard electrical power from a standard electrical receptacle or outlet.

As shown in FIG. 17, the cell phone detector case 150 includes one or more sensor/detector units, cells, or components 176 built into and incorporated into the case 150. The detector 176 includes generally disposed at the front 162 of the case 150 the following types of indicators: a sound alarm indicator 178, a readings panel 180, a sensor 182 for detecting one or more specific types of agents, elements, chemicals, compounds, etc., and a light alarm indicator 184. The sensor/detector 176 will be interconnected to the power source 174. In addition, mounted on and externally visible on the sides 168 or front 162 of the case 150 are a plurality of color coded indicator lights 186 with each light 186 corresponding to a specific agent, element, chemical, compound, etc., and lighting up when that agent

US 9,589,439 B2

13

is detected by the sensor/detector 176. The color coded indicator lights 186 will be electrically interconnected to the sensor/detectors 176 via any standard microprocessor. The cell phone detector case 150 and cell phone monitor 152 thus comprise a hand-held, easily portable and transportable 5 detection means that is both effective and unobtrusive in its disposition and use.

FIGS. 18 and 19 illustrate representative examples of the integration of portable electronic communication or telecommunication devices such as a cell phone 187a and/or a laptop computer 187b with the monitoring equipment 138 10 located at a predesignated monitoring site 188, and operating in conjunction with either a satellite and/or a cell phone tower 190 to transmit and receive signals and commands among each other and to a vehicle 192, such as a truck, as part of a stall-to-stop disabling system for slowing and stopping the vehicle 192 and locking a thief, terrorist, or unauthorized individual in the vehicle 192 if needed. A wide range of events can trigger and initiate the stall-to-stop system and the locking or lock disabling system and mechanism, and the event doesn't have to be limited to the detection of a bomb or a chemical, biological, or radiological agent, element, or compound. The events can include, but is not limited to, detection of an engine problem to engine failure to the unauthorized use (stealing) of the vehicle 192. The vehicle 192 includes an electromotive system 194 that comprises, among other components, an onboard computer(s), electrical, fuel and air systems, as well as brakes, ignition, steering, and transmission. Also integrated with and capable of communicating with the vehicle's 192 electromotive system 194 is a stall-to-stop system while a lock disabling mechanism 196 is able to engage and disengage or disable the vehicle's 192 locking mechanism 198 upon receipt of the appropriate commands via a lock disabling communication channel or link 200. This link 200 20 can also accommodate the stall-to-stop system commands and signals, and thus is a multi-channel communication link. A CPU or a transceiver 202 is programmed to receive signals from the cell phone tower 190 and/or to a GPS satellite 204 and is interconnected with the stall-to-stop system and the lock disabling system 196 via link 200 for engaging the electromotive system 194 and actuating the lock disabling system 196 to stop the vehicle 192 and lock inside the vehicle 192 anyone such as a thief, terrorist or other unauthorized individual.

A representative example for stopping, disabling, and locking the vehicle 192 that utilizes the cell phone tower 190 wherein the activation and/or distress signal 206 originates from the cell phone 187a or the laptop 187b and such activation signal 206 travels to the cell phone tower 190 that is nearest the current location of the vehicle 192. A signal 208 is then transmitted to the monitoring site 188 and specific monitoring equipment 138 that can also include but is not limited to cell phones, laptops, desktop PC's, notebook PC's and LCD monitors. The monitoring site 138 then communicates by signal 210 to the GPS satellite 204 that an original or activation signal has been received and then the GPS satellite 204 locates and communicates by multiplex signal 212 with the CPU or transceiver 202 on the vehicle 192 and exchanges information on the type of problem, situation, location, and vehicle speed. The monitoring equipment 138 then transmits a signal 214 to the cell phone tower 190 that communicates with the transceiver 202 and/or CPU of the vehicle 192 to initiate or execute any commands that will actuate the stall-to-stop disabling link 200 and lock 65 disabling system 196 for bringing the vehicle 192 to a halt and actuating the vehicle's 192 locking mechanism 198 for

14

locking the thief, terrorist, or other unauthorized person inside the vehicle 192 if needed.

FIG. 19 illustrates a representative example wherein the stall-to-stop system and the lock disabling system 196 are utilized in conjunction with the GPS satellite 204. In FIG. 19 a signal has traveled to the satellites nearest the vehicle's 192 current location and then the signal 218 has traveled to the monitoring equipment 138 and monitoring site 188 which can include but is not limited to satellite cell phones, satellite monitors, cell phones, laptops, desktop PC's, notebook PC's, and LCD monitors. The GPS satellite 204 then locates and communicates with the CPU and/or transceiver 202 on the vehicle 192 via a multiplex (two-way) signal 220 in order to exchange information on such distress and danger event parameters as the specific problem situation, location, and vehicle speed. The monitoring equipment 138 then transmits a signal 222 back to the GPS satellite 204 that in turn communicates via another signal 224 with the CPU and/or transceiver 202 to execute any commands to the stall-to-stop system for executing the disengagement of the vehicle's 192 electromotive system 194 for bringing the vehicle 192 to a halt and for actuating the lock disabling system 196 to direct the lock disabling link 200 to actuate the locking mechanism 198 thereby locking the vehicle 192 and anyone inside the vehicle 192.

The present invention comprehends a chemical/biological/radiological/nuclear/explosive/human/contraband detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars, United Parcel Services™ (UPS™), Federal Express™ (FedEx™), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans, unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), and utility vehicles; the products grouped into what may be referred to as Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, door sensors, speed sensors, biometric sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems, detection of humans, detection of contraband, temperature, and shock levels; the products grouped into what may be referred to as Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, suitcases, eyeglass, briefcases, detector cases of locks, detector cases of tags, detector cases that is mounted to, detector cases that is affixed to, detector cases that is outside of, detector cases that is inside of, and detector cases that is adjacent to; the products grouped into what may be referred to as Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, web servers, desktop personal computers (PCs), note-

US 9,589,439 B2

15

book personal computers (PCs), laptops, satellite cell phones, cell phones, Universal Mobile Telecommunications System (UMTS) phones, personal digital assistants (PDAs), liquid crystal display (LCD) monitors, and satellite monitoring, remote control key fobs, two-way communication key fobs, handhelds; the products grouped into what may be referred to as Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Wi-Max, Internet, Ethernet, Broadband, Network Bandwidth, Wireless, Wired, Text Messaging, Cellular, Satellite, Telematics, Wide Area Network (WAN). Wireless Wide Area Network (WWAN), Local Area Network (LAN), Radio Frequency (RF), Broadband Wireless Access (BWA), Global Positioning System (GPS), General Packet Radio Services (GPRS). Global System for Mobile (GSM), Wideband Code Division Multiple Access (W-CDMA), Universal Mobile Telecommunications System (UMTS), Short Message Service (SMS); the products grouped into what may be referred to as Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, band geometry, retina scan, iris scan and signature, the products grouped into what may be referred to as Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside or outside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

While the invention has been shown and described in a preferred embodiment, it will be apparent to those skilled in the art that numerous alterations, modifications, and variations will possible and practicable without departing from the spirit and scope of the invention as set forth by the appended claims.

The invention claimed is:

1. A multi sensor detection system capable of identifying, monitoring, detecting, and securing those critical areas (e.g., U.S. borders), sites, locations and facilities vulnerable to terrorist activity that can be integrated with and interconnected to watchtowers to form a network, comprising:

at least one of an integrated watchtower, a fixed watchtower, a surveillance watchtower, a watchtower capable of scanning, a watchtower capable of monitoring, a watchtower equipped with sensors or a watchtower interconnected to a central monitoring terminal for sending signals thereto and receiving signals therefrom;

wherein the at least one watchtower is equipped with a remote video surveillance camera that provides at least one night vision means of surveillance or an infrared human detection means of surveillance capability and is integrated into a watchtower's remotely controlled system that can monitor, detect, track, and identify humans;

a communication device of at least one of a mobile communication device, a mobile communication unit, a

16

portable communication device, portable communication equipment, a wired communication device, a wireless communication device, a monitoring site, a monitoring terminal, a web server, a desktop personal computer (PC), a notebook personal computer (PC), a laptop, a satellite phone, a smart phone, a cell phone, a Universal Mobile Telecommunications System (UMTS) phone, a personal digital assistant (PDA), a liquid crystal display (LCD) monitor, a satellite, or a handheld, interconnected to a monitoring equipment for sending signals thereto and receiving signals therefrom;

a communication method of at least one of a Bluetooth, Wi-Fi, Wi-Max, Internet, Ethernet, Broadband, Network Bandwidth, Wireless, Wired, Text Messaging, Cellular, Satellite, Telematics, Wide Area Network (WAN), Wireless Wide Area Network (WWAN), Local Area Network (LAN), Radio Frequency (RF), Broadband Wireless Access (BWA), Global Positioning System (GPS), or central processing unit (CPU), used to interconnect the communication device to the monitoring equipment for sending signals thereto and receiving signals therefrom;

a plurality of sensors for detecting or sensing humans that is at least one of a chemical human sensor, biological human sensor, radiological human sensor, infrared human detector, motion human detector, or image human detector, interconnected to or disposed within the multi-sensor detection system for sending signals thereto and receiving signals therefrom;

a mobile multi-sensor detection device that is at least one of a ground surveillance sensor, a surveillance radar sensor, a surveillance camera, or a stand-alone surveillance scanner, that is mounted in, on, or upon at least one of a car, a truck, a camper, a bus, a van, an unmanned aerial vehicle (UAV), an unmanned ground vehicle (UGV), or a utility vehicle, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom;

a hand-held multi-sensor detection device that is capable of at least one of thermal imaging or infrared imaging for monitoring, detecting, tracking and identifying humans, that is controlled or operated by at least one authorized person who is an owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, or monitoring site and terminal personnel, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom, wherein the authorized person manually initiates the signal to the monitoring equipment to alert upon the monitoring, detecting, tracking and identifying of the human;

whereupon, detection by the mobile multi-sensor detection device causes an automatic signal transmission to be sent to, or received from, any products in product grouping categories of storage and transportation, sensors, detector case; modified and adapted, monitoring and communication devices, communication methods, biometrics;

whereupon, detection of an unauthorized vehicle, an unauthorized driver or operator of a vehicle or mobile

US 9,589,439 B2

17

unit, a signal is sent from the communication device to the vehicle or mobile unit to stop, stall or slowdown the vehicle;

wherein, a communication device of at least one of a mobile communication device, a mobile communication unit, a portable communication device, portable communication equipment, a wired communication device, a wireless communication device, a monitoring site, a monitoring terminal, a web server, a desktop PC, a notebook PC, a laptop, a satellite phone, a smart phone, a cell phone, a UMTS phone, a PDA, a LCD monitor, a satellite, or a handheld, interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom, comprising a lock disabling mechanism that is able to engage (lock), and disengage (unlock) and disable (make unavailable) after a specific number of tries.

2. The multi sensor detection system of claim 1, capable of identifying, monitoring, detecting, and securing those critical areas (e.g., U.S. borders), sites, locations and facilities, further includes the identifying, monitoring, and detecting of terrorist, that is at least one of an illegal, radical, fanatic, activist, revolutionist or rebel.

3. The multi-sensor detection system of claim 1, further includes a global positioning system (GPS) receiver adapted for communication with at least one satellite.

4. The multi-sensor detection system of claim 1, further includes a navigation system adapted for communication with at least one of the surveillance watchtowers.

5. The multi-sensor detection system of claim 1, capable of forming a wired or wireless sensor network.

6. The multi-sensor detection system of claim 1, capable of forming a mesh network for redundancy.

7. The multi-sensor detection system of claim 1, capable of transmitting identification data, location data, power source data, and sensor data.

8. The multi-sensor detection system of claim 1, capable of being embedded into; placed in, on, or adjacent to at least one of the products in the product grouping categories or an area targeted for monitoring.

9. The multi-sensor detection system of claim 1, capable of sending signals thereto and receiving signals therefrom to engage (lock), disengage (unlock) and disable (make unavailable) a lock after a specific number of tries that is interconnected to the multi sensor detection system or monitoring equipment.

10. The multi-sensor detection system of claim 1, capable of transmitting biometric and authentication data include, but is not limited to, at least one of fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, heart rate, pulse and signature.

11. The multi-sensor detection system of claim 1, interconnected with a camera to view the environment in real-time or to store the data for transmission and review at a later time.

12. The multi-sensor detection system of claim 1, interconnected with a camera; light and video sensors to allow the user to view the environment from at least one of a cell phone, smart phone, PDA, handheld, laptop, desktop, workstation or monitoring site.

13. A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a personal digital assistant (PDA), a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:

at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor,

18

or a radiological sensor; that is wired or wireless, capable of being disposed within, on, upon or adjacent the communication device;

at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;

a transmitter for transmitting signals and messages to at least one of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;

a receiver for receiving signals, data or messages from at least one of the multi-sensor detection device, the maritime cargo container, the cell phone detection device, or the locking device;

at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;

the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and

whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock locking devices, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;

wherein the communication device receives a signal via any of one or more products in any product grouping categories;

wherein the at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, or short range radio frequency (RF) connection is capable of signal communication with the transmitter, the receiver of the communication device, or transceivers of the products;

wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;

wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, long range radio frequency (RF), and short range radio frequency (RF).

14. Monitoring equipment of at least one of products grouped together by common features in a product groupings category of design similarity comprising a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone interconnected to a product for communication therebetween, the monitoring equipment comprising:

US 9,589,439 B2

19

at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor; that is wired or wireless, capable of being disposed within, on, upon or adjacent the monitoring equipment;

at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;

a transmitter for transmitting signals and messages to at least one of a multi-sensor detection device, a maritime cargo container, a cell phone detection device;

a receiver for receiving signals, data or messages from at least one of the multi-sensor detection device, maritime cargo container, the cell phone detection device;

a lock disabling mechanism that is able to engage (lock), or disengage (unlock), or disable (make unavailable) a product's lock, wherein the lock disabling mechanism disables the product's lock after a specific number of tries by an unauthorized user to disengage the lock by maintaining the product's lock in the current state of the product's lock regardless of input entered to change the state of the product's lock by the unauthorized user;

at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;

monitoring equipment of at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and

whereupon the monitoring equipment, is interconnected to a product equipped to receive signals from or send signals to the lock disabling mechanism that is able to engage, disengage, or disable the lock, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems;

wherein the monitoring equipment is implemented by business or government at a minimum cost by products grouped together by common features in at least one of several product groupings of design similarity;

wherein the at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, or short range radio frequency (RF) connection is in signal communication with the transmitter, the receiver of the monitoring equipment, or transceivers of the products.

15. Monitoring equipment of at least one of the products grouped together by common features in a product groupings category of design similarity comprising a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone interconnected to a product for communication therebetween, the monitoring equipment comprising:

at least one of a central processing unit (CPU), a network processor, or a microprocessor for executing and carrying out the instructions of a computer program or application which is specifically targeted at the networking application domain, for communication between the monitoring equipment and at least one of

20

a multi-sensor detection device, a maritime cargo container device, or a locking device;

a transmitter for transmitting signals and messages to at least one of the multi-sensor detection device, the maritime cargo container device, or the locking device;

a receiver for receiving signals, data or messages from at least one of the multi-sensor detection device, the maritime cargo container device or the locking device, wherein the signals, data or messages are of agents of an item of interest (IOI);

at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, or GPS connection;

the monitoring equipment is at least a fixed, portable or mobile monitoring equipment interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween; and

whereupon the monitoring equipment, is capable of the activation or deactivation of at least one of the multi-sensor detection device, the maritime cargo container device or the locking device;

wherein the at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, for signal communication with the transmitter, the receiver of the monitoring equipment, or transceivers of the products;

at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of a chemical agent, a biological agent, a radiological agent, a nuclear agent, or an explosive agent which allows radio frequency (RF) data to be at least one of received or transmitted between the tag and the monitoring equipment.

16. A built-in, embedded multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents;

comprising a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor;

comprising a communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a personal digital assistant (PDA), a laptop, or a computer terminal for monitoring products, interconnected to a built-in sensor array or fixed detection device for communication therebetween;

wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan or signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use;

wherein the built-in embedded multi-sensor detection device receives a signal via any of one or more products in any product grouping categories; and

wherein, when an alarm occurs, the built-in, embedded multi sensor detection system communicates the alarm by way of at least one of the products grouped together

US 9,589,439 B2

21

by common features in a product groupings category of design similarity comprising at least one of product-to-product, product-to-satellite, product-to-cellular, product-to-long range radio frequency, product-to-short range radio frequency, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop for communication therebetween;

wherein the built-in embedded multi-sensor detection device is implemented by business or government at a minimum cost by products grouped together by common features in at least one of the several product groupings of design similarity.

17. A built-in multi sensor detection system for monitoring products with a plurality of sensors detecting at least two agents selected from the group consisting of chemical, biological, radiological, explosive, human, and contraband agents, comprising:

a built-in sensor array or fixed detection device into the product that detects agents by means of two or more sensors combined from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor;

monitoring equipment of at least one of products grouped together by common features in a product groupings category of design similarity comprising at least one of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone for the receipt and transmission of signals therebetween;

wherein the built-in multi-sensor detection device is built in any of one or more products comprising a maritime cargo container, a lock, or the monitoring equipment; wherein the built-in multi-sensor detection device is implemented by business or government by products grouped together by common features in at least one of several product groupings of design similarity;

a light alarm indicator that has a plurality of colored lights that correspond to specific agents of the at least two agents;

wherein, when the light alarm indicator lights to indicate an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in the product groupings category of design similarity comprising at least one of product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop for at least one of a receipt or transmission of signals therebetween.

18. A built-in multi sensor detection system for detecting at least two items selected from the group consisting of chemical agent, biological agent, radiological agent, explosive agent, human agent, contraband agent, motion, perimeter, temperature, tampering, theft, or breach, comprising:

a built-in sensor array or fixed detection device into a product that detects items by means of at least two sensors from the following list of sensors: a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor;

22

monitoring equipment of at least one of the products grouped together by common features in a product groupings category of design similarity comprising at least one of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone for the receipt and transmission of signals therebetween;

wherein the built-in, multi-sensor detection device is built in any of one or more products comprising a maritime cargo container, a lock, or the monitoring equipment; wherein, when an alarm occurs, the built-in multi sensor detection system communicates the alarm by way of at least one of the products grouped together by common features in a product groupings category of design similarity comprising at least one of product-to-product, product-to-satellite, product-to-cellular, product-to-radio frequency (RF), product-to-internet, product-to-broadband, product-to-smartphone or cell phone, product-to-computer at monitoring site, product-to-WiFi, product-to-handheld, or product-to-laptop or desktop for the receipt and transmission of signals therebetween;

at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of the chemical agent, the biological agent, the radiological agent, the explosive agent, the human agent, the contraband agent, the motion, the perimeter, the temperature, the tampering, the theft, and the breach which allows radio frequency (RF) data to be received and/or transferred between the tag and the monitoring equipment.

19. A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, radiological agent, or compound, comprising:

a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human, or contraband agent or compound, capable of being disposed within, on, upon or adjacent a multi-sensor detection device;

monitoring equipment comprising at least one of a computer, personal computer (PC), laptop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone for at least one of a receipt or transmission of signals therebetween;

at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom or at least one satellite capable of transmitting signals to the monitoring equipment;

at least one satellite or at least one cell phone tower capable of signal communication between the multi-sensor detection device and the monitoring equipment;

at least one internet connection capable of communication between the multi-sensor detection device and the monitoring equipment;

whereupon a signal sent to a receiver of the multi-sensor detection device from a satellite; or to a cell phone tower; or through at least one of a short range radio frequency or a long range radio frequency; causes a signal to be sent to the monitoring equipment that includes at least one of location data or sensor data;

wherein the monitoring equipment or multi-sensor detection device receives a signal via any of one or more products of any product grouping categories;

wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection,

US 9,589,439 B2

23

radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency connection, or short range radio frequency (RF) connection is capable of signal communication with the transmitter, a receiver of the monitoring equipment, the multi-sensor detection device, or transceivers of the products; wherein the monitoring equipment is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan or signature such that the monitoring device that is at least one of the computer, the laptop, the notebook, the PC, the handheld, the cell phone, the PDA, or the smart phone is locked by the biometric lock disabler to prevent unauthorized use; wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, long range radio frequency, and short range radio frequency (RF).

20. A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, radiological agents or compound, comprising:

a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human, or contraband agent or compound, capable of being disposed within, on, upon or adjacent a multi-sensor detection device;

monitoring equipment of at least one of products grouped together by common features in a product groupings category of design similarity comprising at least one of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA), or smart phone for at least one of a receipt or transmission of signals therebetween,

wherein the monitoring equipment is equipped with a lock disabling mechanism that is able to engage (lock), or disengage (unlock), or disable (to make unavailable) a product's lock, wherein the lock disabling mechanism disables the product's lock after a specific number of tries by an unauthorized user to disengage the lock by maintaining the product's lock in the current state of the product's lock regardless of input entered to change the state of the product's lock by the unauthorized user;

at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom; or at least one satellite capable of transmitting signals to the monitoring equipment;

at least one satellite or at least one cell phone tower capable of signal communication between the multi-sensor detection device and the monitoring equipment;

at least one internet connection capable of communication between the multi-sensor detection device and the monitoring equipment; and

whereupon a signal sent to a receiver of the multi-sensor detection device from a satellite; or to a cell phone tower; or through at least one of a short range radio frequency or a long range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and/or sensor data;

wherein the multi-sensor detection device is implemented by business or government by products grouped together by common features in at least one of several product groupings of design similarity;

24

wherein the multi-sensor detection device is for any of one or more products comprising a maritime cargo container, a lock, or the monitoring equipment;

wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency connection, or short range radio frequency connection is in signal communication with a transmitter and a receiver of the monitoring equipment or multi-sensor detection device and transceivers of the products.

21. A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:

a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human, or contraband agent or compound, capable of being disposed within, on, upon or adjacent a multi-sensor detection device, wherein at least one of the sensors is capable of detecting agents of an item of interest (IOI); monitoring equipment of at least one of the products grouped together by common features in a product groupings category of design similarity comprising at least one of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA), or smart phone for at least one of a receipt or transmission of signals therebetween;

at least one satellite or at least one cell phone tower capable of signal communication between the multi-sensor detection device and the monitoring equipment;

at least one internet connection capable of communication between the multi-sensor detection device and the monitoring equipment;

whereupon a signal sent to a receiver of the multi-sensor detection device for detecting the agents of the item of interest causes a signal that includes at least one of location data or sensor data to be sent to the monitoring equipment;

wherein the multi-sensor detection device for any of one or more products comprising a maritime cargo container, a lock, or the monitoring equipment;

wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, or broadband connection, is in signal communication with a transmitter, a receiver of the monitoring equipment, or transceivers of the products;

at least one tag that is read by the monitoring equipment that is capable of wireless near-field communication to achieve detection of at least one of the explosive agent, the nuclear agent, the contraband agent, the chemical agent, the biological agent, the human agent, or the radiological agent which allows radio frequency (RF) data to be received and/or transferred between the tag and the monitoring equipment.

22. A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a personal digital assistant (PDA), a laptop, or a computer terminal, comprising:

at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor; that is wired or wireless, capable of being disposed within, on, upon or adjacent the communication device;

US 9,589,439 B2

25

at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between a host computer and other devices;

a transmitter for transmitting signals and messages to at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;

a receiver for receiving signals, data or messages from at least one of a multi-sensor detection device, a cell phone detection device, or a locking device;

at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long and/or short range radio frequency (RF) connection, or GPS connection;

the communication device being at least a fixed, portable or mobile communication device, equipped with at least one wired or wireless sensor for the detection of humans;

the communication device being equipped to receive signals from or send signals to engage (lock), disengage (unlock), or disable (make unavailable) locks;

the communication device being equipped with biometrics that incorporates at least one of a fingerprint recognition or a face recognition to at least one of gain access to the device or to prevent unauthorized use;

the communication device being capable of wireless near-field communication (NFC) which allows radio frequency (RF) data to be at least one of received or transferred between the communication device and at least one tag that is read by the communication device;

whereupon a signal sent to the receiver of at least one of a multi-sensor detection device, a cell phone detection device, or a locking device from a satellite or a cell phone tower or through at least one of a Bluetooth connection, a WiFi connection, an internet connection, a cellular connection, a GPS connection, a short range radio frequency (RF) connection, or a long range radio frequency (RF) connection, causes a signal that includes at least one of location data or sensor data to be sent to the communication device; and

wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long range radio frequency (RF) connection, or short range radio frequency (RF) connection, capable of signal communication with the transmitter of the communication device, the receiver of the communication device, or the central processing unit (CPU).

26

23. A cell phone comprising:

a central processing unit (CPU) for executing and carrying out the instructions of a computer program;

a transmitter for transmitting signals and messages to a cell phone detection device;

a receiver for receiving signals from the cell phone detection device;

at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;

the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and

whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi-sensor detection systems, or to activate or deactivate the cell phone detection device;

at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;

wherein at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection is capable of signal communication with the transmitter or the receiver;

wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and

whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.

* * * * *

(12) **United States Patent**
Golden

(10) **Patent No.:** **US 10,163,287 B2**

(45) **Date of Patent:** **Dec. 25, 2018**

(54) **MULTI SENSOR DETECTION, STALL TO STOP AND LOCK DISABLING SYSTEM**

9/00563; G08B 27/00; G08B 27/005;
G08B 27/006; B60R 25/018; B60R
25/04; B60R 25/10; B50R 25/102

(71) Applicant: **Larry Golden**, Greenville, SC (US)

See application file for complete search history.

(72) Inventor: **Larry Golden**, Greenville, SC (US)

(56)

References Cited

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

U.S. PATENT DOCUMENTS

4,385,469 A 5/1983 Scheuerpflug et al.
4,544,267 A 10/1985 Schiller

(Continued)

(21) Appl. No.: **15/530,839**

(22) Filed: **Mar. 6, 2017**

OTHER PUBLICATIONS

(65) **Prior Publication Data**

US 2017/0186259 A1 Jun. 29, 2017

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/199,853; copyright and dated Jan. 13, 2012, pp. 1-34, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (34 pages).

(Continued)

Related U.S. Application Data

(60) Continuation of application No. 14/806,988, filed on Jul. 23, 2015, now Pat. No. 9,589,439, which is a continuation of application No. 14/021,693, filed on Sep. 9, 2013, now Pat. No. 9,096,189, which is a continuation of application No. 13/288,065, filed on Nov. 3, 2011, now Pat. No. 8,531,280, which is a
(Continued)

Primary Examiner — Van Trieu

(57)

ABSTRACT

A multi sensor detection and disabling lock system includes detector cases for holding interchangeable detectors that sample for chemical, biological and radiological compounds, agents and elements, with each detector case disposed in or upon the monitored product. The detector case transmits detection information to a monitoring computer terminal and transmits a signal to a lock disabler engaged to the product to lock or disable the product's lock thereby preventing untrained, unauthorized and unequipped individuals from gaining access and entry to the product, and also preventing further contamination of the area. The detection system can be interconnected to surveillance towers scanning detector cases disposed at seaport docks, freight depots and rail terminals for monitoring containers being prepared for shipment or sitting on docks for long periods of time.

(51) **Int. Cl.**

G08B 27/00 (2006.01)

G07C 9/00 (2006.01)

B60R 25/24 (2013.01)

B60R 25/04 (2013.01)

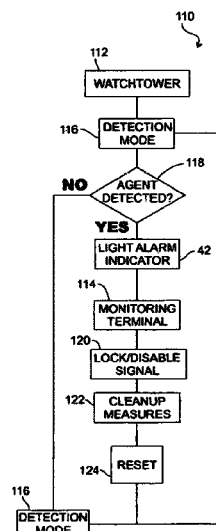
(52) **U.S. Cl.**

CPC **G07C 9/00174** (2013.01); **B60R 25/04** (2013.01); **B60R 25/24** (2013.01); **G07C 9/00007** (2013.01); **G07C 9/00563** (2013.01)

(58) **Field of Classification Search**

CPC .. **G07C 9/00**; **G07C 9/00007**; **G07C 9/00174**;
G07C 9/00309; **G07C 9/00388**; **G07C**

6 Claims, 13 Drawing Sheets



US 10,163,287 B2

Page 2

Related U.S. Application Data

division of application No. 12/802,001, filed on May 27, 2010, now Pat. No. 8,334,761, which is a continuation of application No. 12/657,356, filed on Jan. 20, 2010, now Pat. No. 8,106,752, which is a continuation of application No. 12/155,573, filed on Jun. 6, 2008, now Pat. No. 7,636,033, which is a continuation-in-part of application No. 11/397,118, filed on Apr. 5, 2006, now Pat. No. 7,385,497.

(56)

References Cited

U.S. PATENT DOCUMENTS

4,586,441	A	5/1986	Zekich
4,792,226	A	12/1988	Fishbine et al.
5,222,152	A	6/1993	Fishbine et al.
5,223,844	A	6/1993	Mansell et al.
5,233,404	A	8/1993	Lougheed et al.
5,557,254	A	9/1996	Johnson et al.
5,682,133	A	10/1997	Johnson et al.
5,766,956	A	6/1998	Groger et al.
5,938,706	A	8/1999	Feldman
5,959,529	A	9/1999	Kail
5,963,657	A	10/1999	Bowker et al.
5,986,543	A	11/1999	Johnson
5,990,785	A	11/1999	Suda
6,049,269	A	4/2000	Byrd et al.
6,078,265	A	6/2000	Bonder et al.
6,262,656	B1	7/2001	Byrd et al.
6,271,745	B1	8/2001	Anzai et al.
6,374,652	B1	4/2002	Hwang
6,411,887	B1	6/2002	Martens et al.
6,470,260	B2	10/2002	Martens et al.
6,542,076	B1	4/2003	Joao
6,542,077	B2	4/2003	Joao
6,588,635	B2	7/2003	Vor Keller et al.
6,610,977	B2	8/2003	Megerle
6,613,571	B2	9/2003	Cordery et al.
6,628,813	B2	9/2003	Scott et al.
6,647,328	B2	10/2003	Walker
6,738,697	B2	5/2004	Breed
6,923,509	B1	8/2005	Barnett
6,980,092	B2	12/2005	Turnbull et al.
6,988,026	B2	1/2006	Breed et al.
7,005,982	B1	2/2006	Frank
7,034,677	B2	4/2006	Steinthal et al.
7,034,683	B2	4/2006	Ghazarian
7,103,460	B1	9/2006	Breed
7,116,798	B1	10/2006	Chawla
7,148,484	B2	12/2006	Craig et al.
7,171,312	B2	1/2007	Steinthal et al.
7,184,117	B2	1/2007	Breed et al.
7,243,945	B2	7/2007	Breed et al.
7,339,469	B2	3/2008	Braun
7,346,439	B2	3/2008	Bodin
7,350,608	B2*	4/2008	Fernandez B60L 1/00 180/65.1
7,385,497	B2	6/2008	Golden
7,397,363	B2	7/2008	Joao
7,636,033	B2	12/2009	Golden
7,647,180	B2	1/2010	Breed
7,844,505	B1	11/2010	Arneson et al.
7,868,912	B2	1/2011	Venetianer et al.
7,872,575	B2	1/2011	Taba
7,880,767	B2	2/2011	Chinigo
7,961,094	B2	6/2011	Breed
8,120,459	B2*	2/2012	Kwak G07C 9/00309 340/5.2
8,274,377	B2	9/2012	Smith et al.
8,531,521	B2	9/2013	Romanowich
8,564,661	B2	10/2013	Lipton et al.
2002/0145666	A1	10/2002	Scaman
2003/0063004	A1	4/2003	Anthony et al.
2003/0137426	A1	7/2003	Anthony et al.
2003/0179073	A1*	9/2003	Ghazarian E05B 47/00 340/5.6

2003/0206102	A1	11/2003	Joao
2004/0107028	A1	6/2004	Catalano
2004/0222092	A1	11/2004	Musho
2005/0195069	A1	9/2005	Dunand
2006/0164239	A1	7/2006	Loda
2006/0176169	A1	8/2006	Doolin et al.
2006/0181413	A1	8/2006	Mostov
2006/0250235	A1	11/2006	Astrin
2007/0093200	A1*	4/2007	Dobosz H04B 7/18565 455/3.02
2007/0171042	A1	7/2007	Metes et al.
2007/0257774	A1*	11/2007	Stumpert G06Q 10/08 340/7.1
2008/0045156	A1	2/2008	Sakhpara
2008/0122595	A1	5/2008	Yamamichi et al.
2008/0234907	A1	9/2008	Labuhn et al.
2010/0159983	A1	5/2010	Golden
2011/0178655	A1	6/2011	Golden

OTHER PUBLICATIONS

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and dated Dec. 2, 2011, pp. 1-27, publisher United States and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (27 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and dated Nov. 1, 2011, pp. 1-18, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (18 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 11/397,118; dated Nov. 14, 2007; Alexandria, Virginia, USA; pp. 1-12; U.S. Appl. No. 13/288,065 (12 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/155,573; dated Apr. 9, 2009; Alexandria, Virginia, USA; pp. 1-7; U.S. Appl. No. 13/288,065 (7 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/155,573; dated Jul. 30, 2009; Alexandria, Virginia, USA; pp. 1-9; U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Notice of Allowability from U.S. Appl. No. 12/155,573; dated Oct. 28, 2009; Alexandria, Virginia, USA; pp. 1-5; U.S. Appl. No. 13/288,065 (5 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/657,356; dated Jul. 12, 2010; Alexandria, Virginia, USA; pp. 1-14; U.S. Appl. No. 13/288,065 (14 pages).

United States Patent and Trademark Office; Notice of Allowability from U.S. Appl. No. 12/657,356; dated Mar. 10, 2011; Alexandria, Virginia, USA; pp. 1-4; U.S. Appl. No. 13/288,065 (4 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 13/065,837; dated Jul. 18, 2011; Alexandria, Virginia, USA; pp. 1-9; U.S. Appl. No. 13/288,065 (9 pages).

A newspaper article of Mr. Melvin Sullivan and his family that references the date, Mar. 5, 2001, U.S. Appl. No. 13/288,065.

A letter of response Mr. Sullivan received from Pfeiffer & Gantt, PA, dated Sep. 16, 2002, U.S. Appl. No. 13/288,065.

A "Certificate of Existence" Bright Idea Inventor, LLC. Nov. 6, 2002, U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Congressman from Maryland, Elijah E. Cummings, dated Dec. 16, 2002; U.S. Appl. No. 13/288,065.

A newspaper article of Mr. Melvin Sullivan and Mr. Larry Golden, dated Feb. 27-Mar. 5, 2003; U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated May 21, 2003; U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Office of the Vice President, Dick Cheney, dated Jun. 3, 2003; U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated Oct. 1, 2003; U.S. Appl. No. 13/288,065.

A letter of response Golden received from the Honorable Senator from South Carolina, Lindsey O. Graham, dated Oct. 21, 2003; U.S. Appl. No. 13/288,065.

US 10,163,287 B2

Page 3

(56)

References Cited

OTHER PUBLICATIONS

A letter sent to the President of the United States George W Bush, the President's Cabinet, the United States Senate and the Congressional Black Caucus, dated May 23, 2005; U.S. Appl. No. 13/288,065. On Nov. 17, 2005, an "Inventor's Office Record of Invention", was filed in my name (Golden) at "The Law Office of David P. Gaudio, P.C.; the Inventors Network."; U.S. Appl. No. 13/288,065. On Aug. 23, 2005, the "Disclosure Document Registration"; U.S. Appl. No. 13/288,065.

On Apr. 5, 2006, the "Patent Application" was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; U.S. Appl. No. 13/288,065.

On Jun. 6, 2008, the "Continuance-In-Part, (CIP) Application" was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; U.S. Appl. No. 13/288,065.

On Jan. 20, 2010, a "Continuation Application" (U.S. Appl. No. 12/657,356) was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; U.S. Appl. No. 13/288,065.

Reissue of U.S. Pat. No. 7,636,033, "Swear Back"; in accordance to Title 37—Code of Federal Regulations Patents, Trademarks, and Copyrights; Apr. 8, 2011; U.S. Appl. No. 13/288,065.

Reissue of U.S. Pat. No. 7,636,033; "Swearback-History of Work"; Apr. 8, 2011; U.S. Appl. No. 13/288,065.

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001, dated Apr. 14, 2011, 2011; Alexandria, Virginia, USA; pp. 1-16; U.S. Appl. No. 13/288,065 (16 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; dated May 27, 2011; Alexandria, Virginia, USA; pp. 1-14, U.S. Appl. No. 13/288,065 (14 pages).

United States Department of Homeland Security: Petition for Inter Partes Review of U.S. Pat. No. Re. 43,990 Under 35 U.S.C. §312 and 37 C.F.R. §42.104; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-57; U.S. Appl. No. 14/806,988 (57 pages).

United States Department of Homeland Security; Declaration of Dr. Sriram Vishwanath; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington D.C., USA; pp. 1-44; U.S. Appl. No. 14/806,988 (44 pages).

Richard R Brooks and S.S. Iyengar; Multi-Sensor Fusion Fundamentals and Applications with Software; published 1998; Copyright Prentice Hall PTR; Upper Saddle River, New Jersey, USA; pp. 1-20; copy enclosed (20 pages), U.S. Appl. No. 14/806,988 (20 pages). Ramanarayanan Viswanathan and Pramod K Varshney; Distributed Detection with Multiple Sensors: Part I—Fundamentals; Proceedings of the IEEE; Jan. 1, 1997; pp. 1-11; vol. 85; No. 1; Southern Illinois University Carbondale OpenSIUC; Illinois, USA; pp. 1-11; U.S. Appl. No. 14/806,988 (11 pages).

Blum; Distributed Detection with Multiple Sensors: Part II—Advanced Topics; Proceedings of the IEEE; Jan. 1, 1997; pp. 1-16; vol. 85, No. 1; Southern Illinois University Carbondale OpenSIUC; Illinois, USA; U.S. Appl. No. 14/806,988 (16 pages).

Victor Lesser; Distributed Sensor Networks a Multisensor Perspective; 2003; pp. 1, 2, 5, 6322, 26, 27, 36, 275, 320; copyright 2003 Kluwer Academic Publishers; AH Dordrecht, The Netherlands; U.S. Appl. No. 14/806,988 (10 pages).

Samuel Blackman and Robert Popoli; Design and Analysis of Modern Tracking Systems; 1999; pp. 1, 2, 6, 472; copyright 1999 Artech House; Norwood, Massachusetts, USA; U.S. Appl. No. 14/806,988 (4 pages).

Jean-Francois Chamberland; Decentralized Detection in Sensor Networks; 2003; pp. 407-416 IEEE Transactions on Signal Processing; vol. 51, No. 2; Urbana, Illinois, USA; U.S. Appl. No. 14/806,988 (10 pages).

Oleg Kachirski and Ratan Guha; Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks; pp. 1-8; Proceedings of the 36th Hawaii International Conference on System Sciences; copyright 2003; Orlando, Florida, USA; U.S. Appl. No. 14/806,988 (8 pages).

Lawrence A Klein; Sensor and Data Fusion a Tool for Information Assessment and Decision Making; 2004; pp. 1-4, 6, 81, 87-89; copyright 2004 The Society of Photo-Optical Instrumentation Engineers; Publisher is SPIE—the International Society for Optical Engineering; Bellingham, Washington, USA; U.S. Appl. No. 14/806,988.

Dale Ferriere and Khrystyna Pysareva and Andrzej Rucinski; Using Technology to Bridge Maritime Security Gaps; Aug. 1, 2005; Sea Technology; pp. 1-6; copyright Compass Publications, Inc. Jan. 2009; Portsmouth, New Hampshire, USA; U.S. Appl. No. 14/806,988 (6 pages).

Corie Lok; Cargo Security; MIT Technology Review; Jun. 2004; No. 107; pp. 74-75; publisher is Massachusetts Institute of Technology; Cambridge, Massachusetts, USA; USPASN14/806988 (2 pages).

Thomas C Chen; RFID and Sensor-based Container Content Visibility and Seaport Security Monitoring system; Proceedings of SPIE, vol. 5778; pp. 151-159; Mar. 28, 2005; Publisher is SPIE—the International Society for Optical Engineering; Bellingham, Washington, USA; USPASN14/806988 (10 pages).

United States Department of Homeland Security; The University of Texas at Austin College of Engineering Standard Resume of Sriram Vishwanath; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-21; USPASN14/806988 (21 pages).

Operating Agreement of Bright Idea Inventor, LLC received from Pfeiffer & Gantt, PA, dated Nov. 13, 2002; U.S. Appl. No. 13/288,065. United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; dated Oct. 20, 2011; Alexandria, Virginia, USA; pp. 1-5; parent U.S. Appl. No. 13/288,065 (5 pages); U.S. Appl. No. 13/288,065 (5 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802,001; copyright and dated Dec. 12, 2011, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA, parent U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802,001; copyright and dated Mar. 26, 2012, pp. 1-12, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (12 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/199,853; copyright and dated Feb. 22, 2012, pp. 1-38, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (38 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright and dated Feb. 22, 2012, pp. 1-25, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA, U.S. Appl. No. 13/288,065 (25 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and dated Aug. 24, 2012, pp. 1-4, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (4 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and dated Nov. 28, 2012, pp. 1-11, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (11 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright and dated Apr. 16, 2013, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright and dated Apr. 20, 2015, pp. 1-20, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 14/021,693 (20 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright and dated Jan.

US 10,163,287 B2

Page 4

(56)

References Cited

OTHER PUBLICATIONS

20, 2015, pp. 1-17, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 14/021,693 (17 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright and dated Sep. 5, 2014, pp. 1-12, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 14/021,693 (12 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/806,988; copyright and dated Jul. 5, 2015, pp. 1-5, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 14/806,988 (5 pages).

United States Patent and Trademark Office; Notice of Allowance from U.S. Appl. No. 14/806,988; dated Jan. 3, 2017; Alexandria, Virginia, USA; pp. 1-8; U.S. Appl. No. 14/806,988 (8 pages).

United States Patent and Trademark Office; Notice of Allowance from U.S. Appl. No. 14/021,693; dated Jun. 19, 2015; Alexandria, Virginia, USA; pp. 1-8; U.S. Appl. No. 14/021,693 (8 pages).

United States Patent and Trademark Office; Notice of Allowance from U.S. Appl. No. 13/288,065; dated May 24, 2013; Alexandria, Virginia, USA; pp. 1-8; U.S. Appl. No. 13/288,065 (8 pages).

* cited by examiner

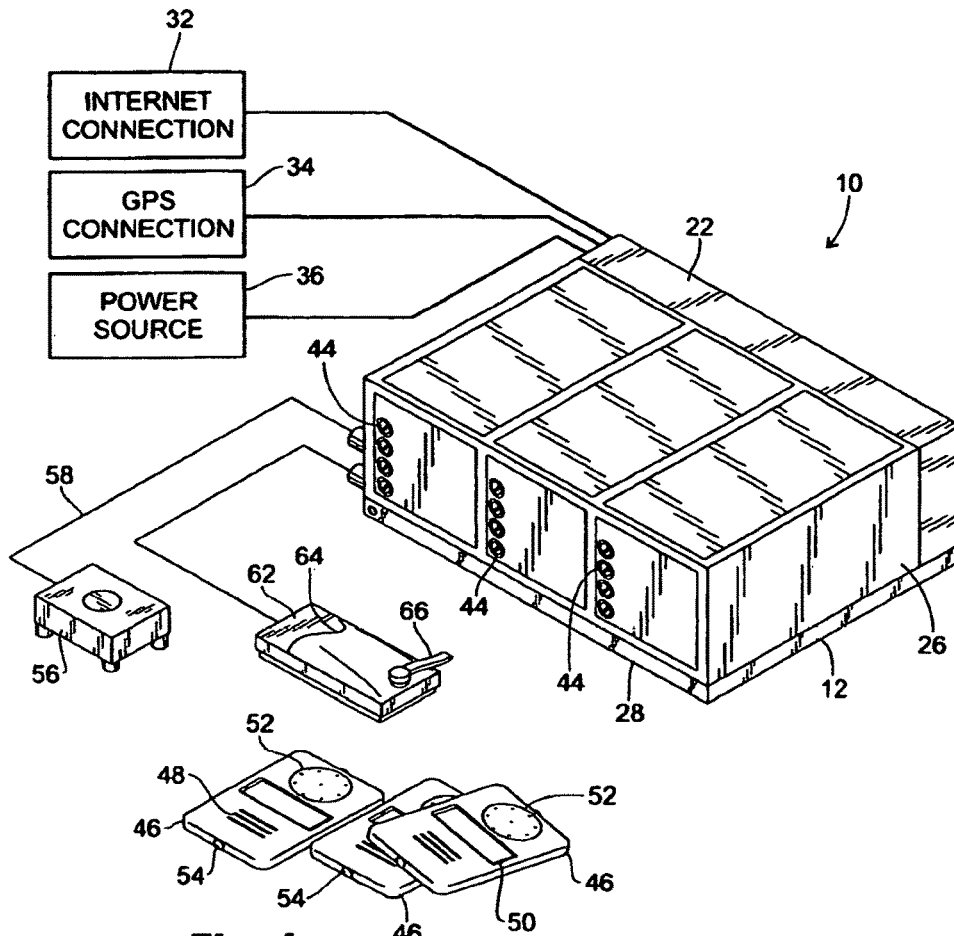


Fig. 1

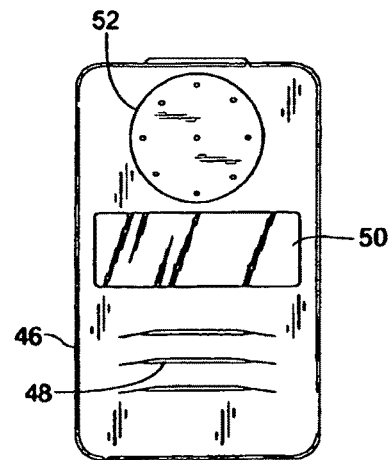


Fig. 2

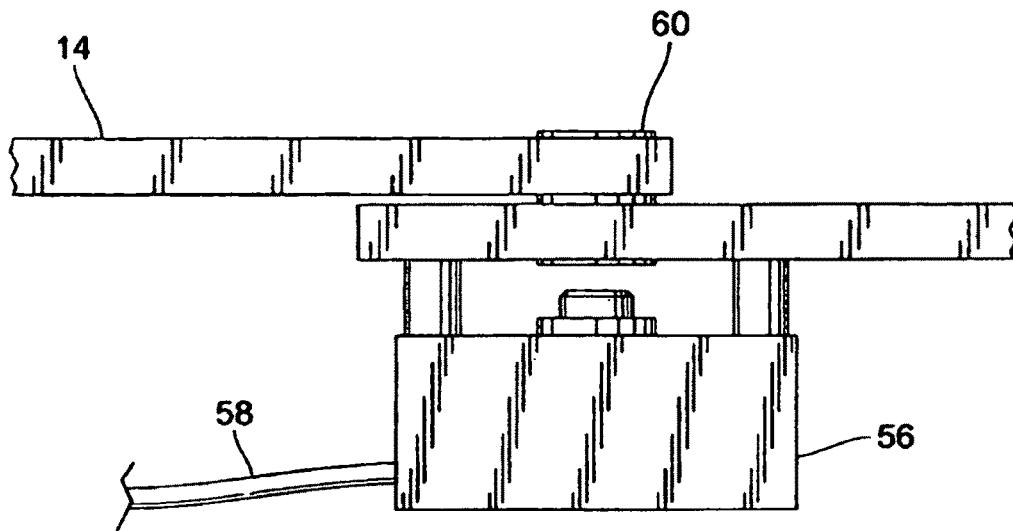


Fig. 3a

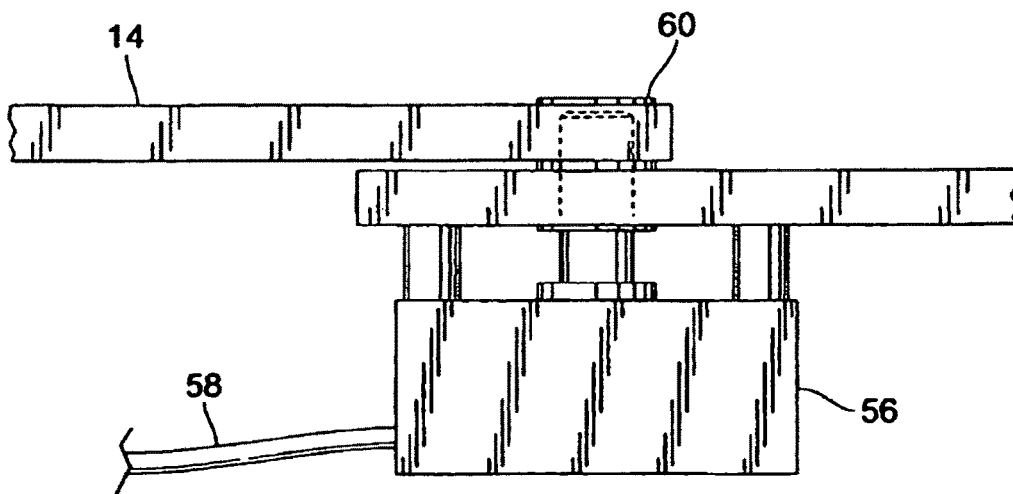


Fig. 3b

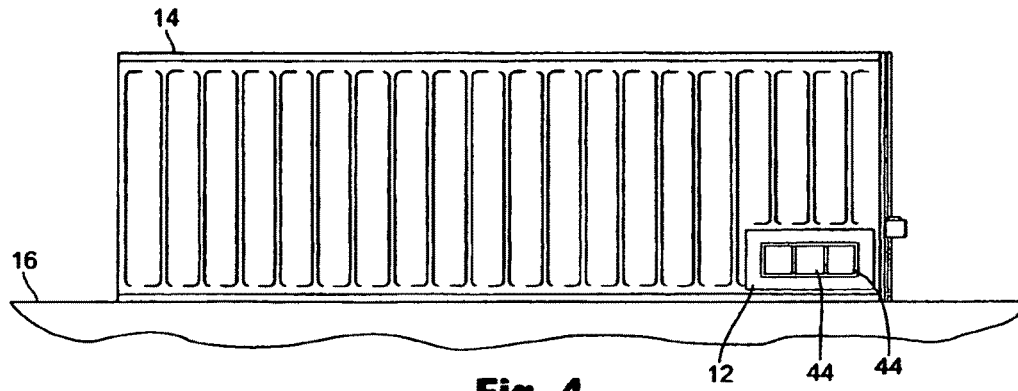


Fig. 4

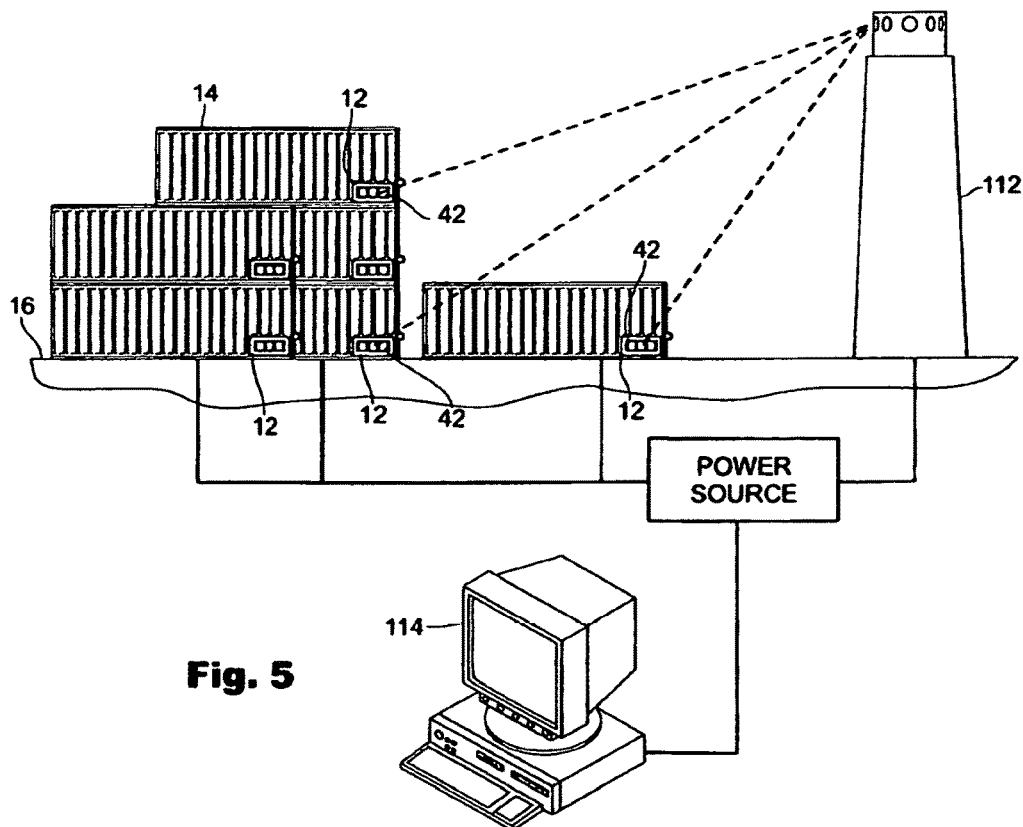


Fig. 5

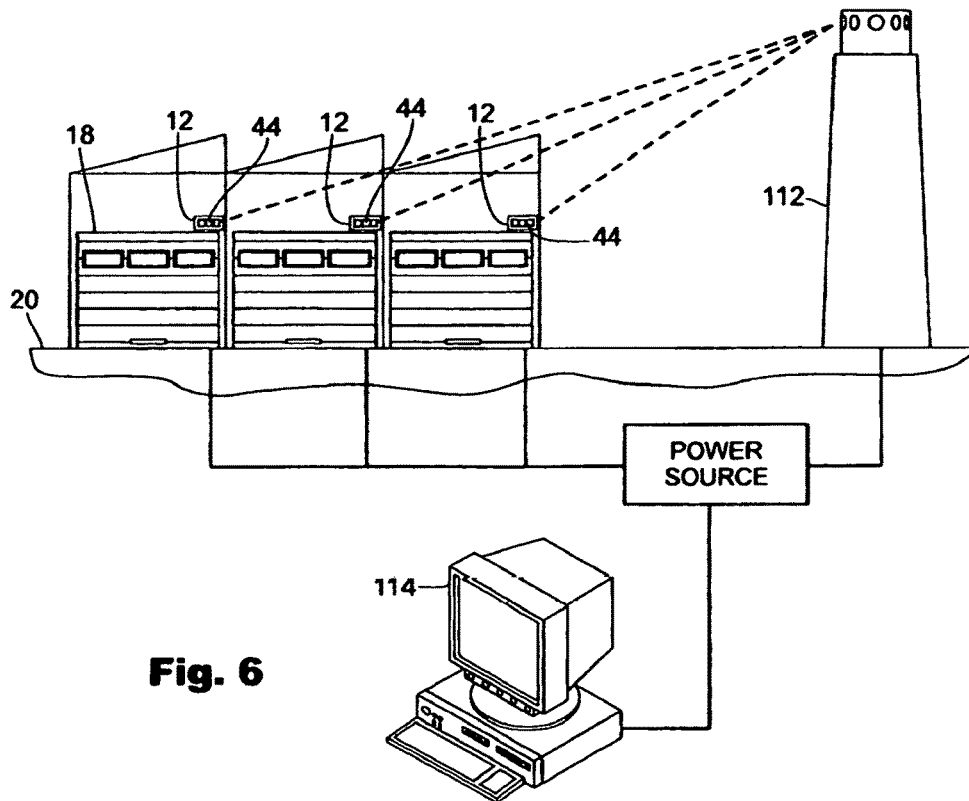


Fig. 6

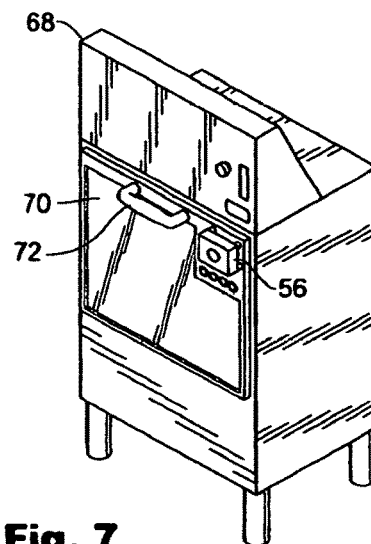


Fig. 7

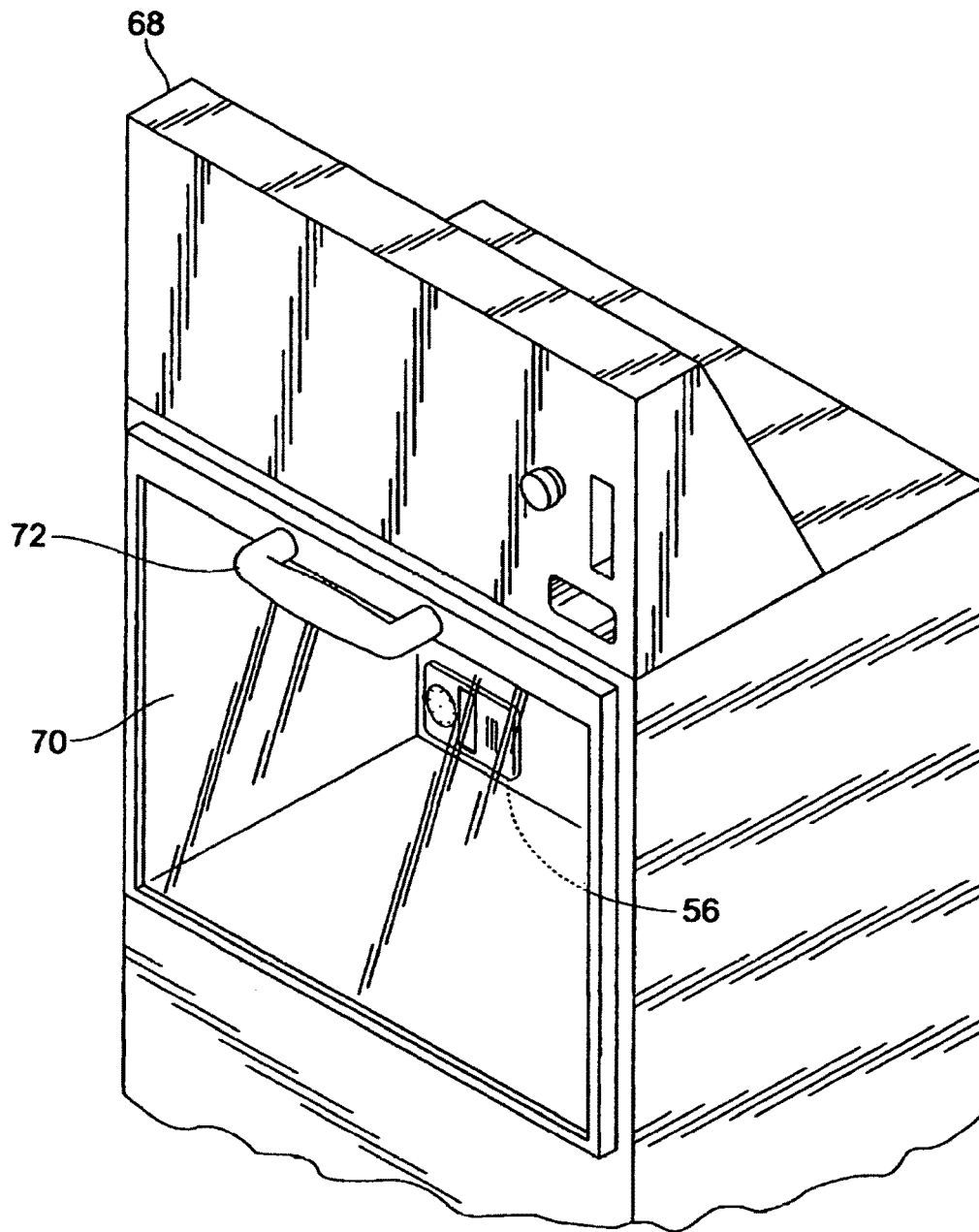


Fig. 8

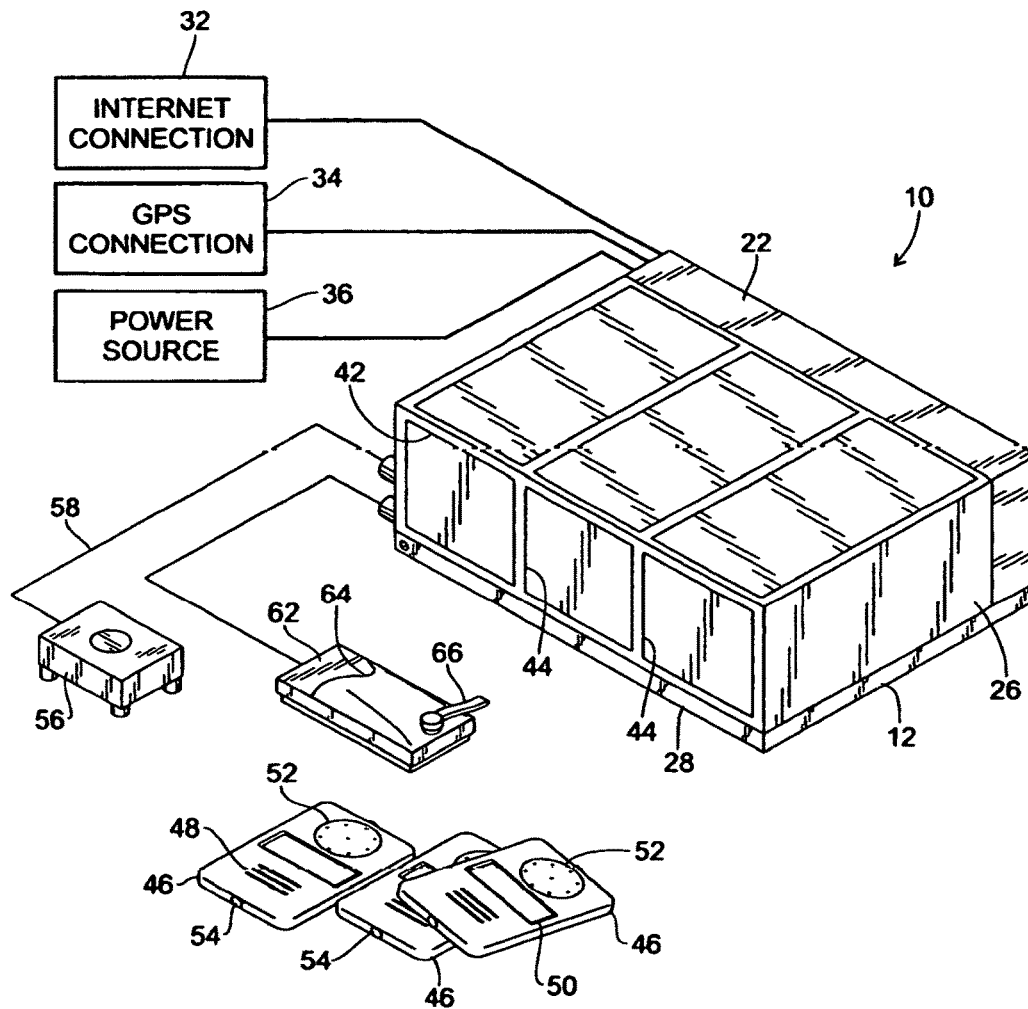


Fig. 9

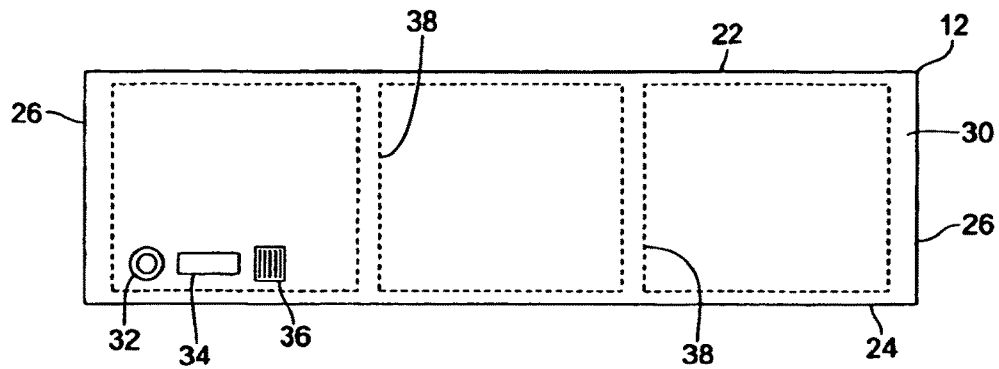


Fig. 10

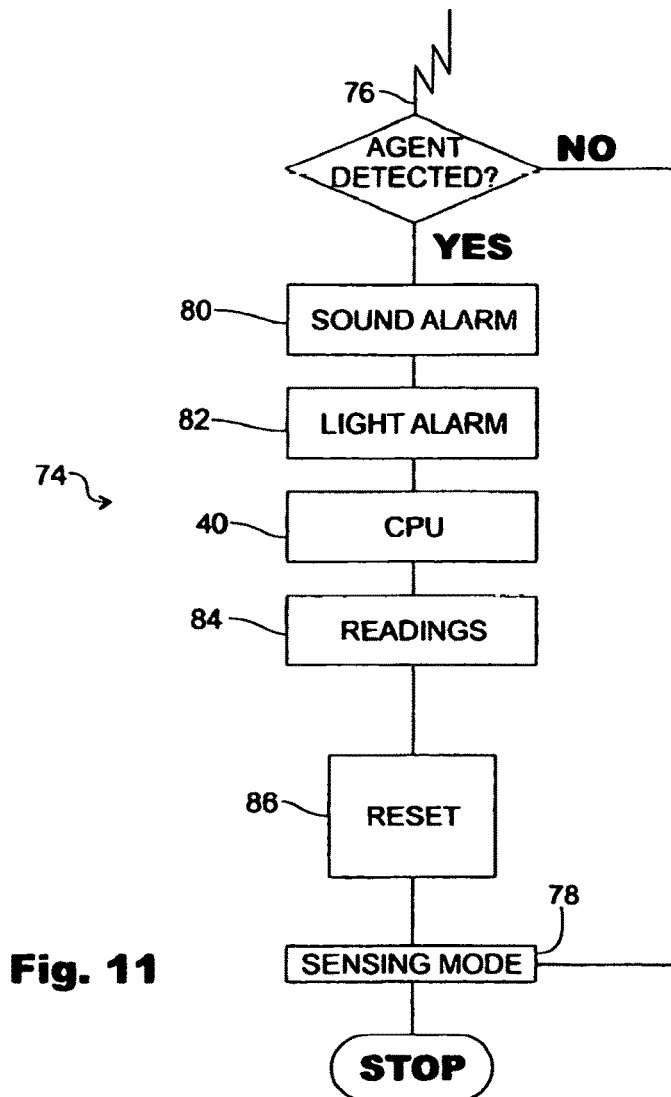


Fig. 11

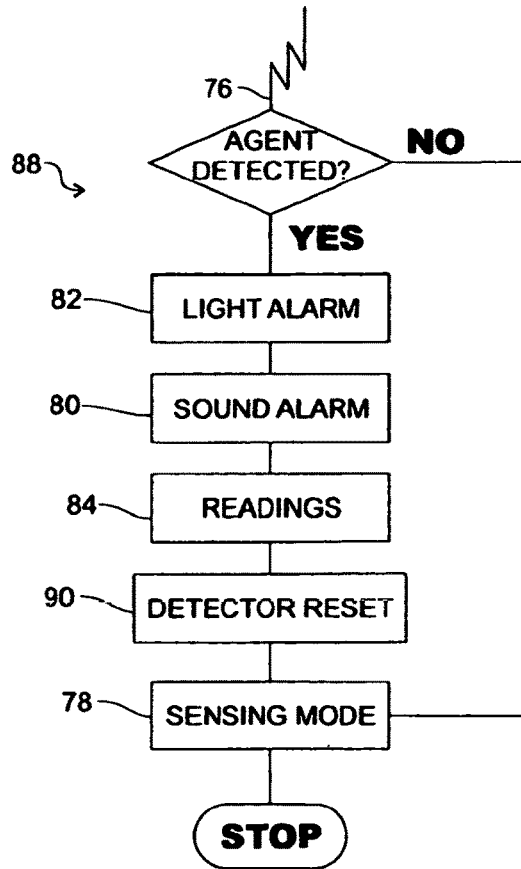


Fig. 12

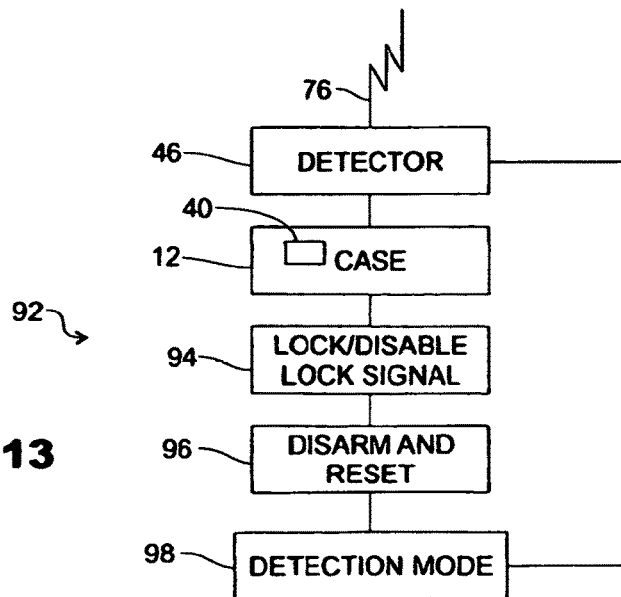
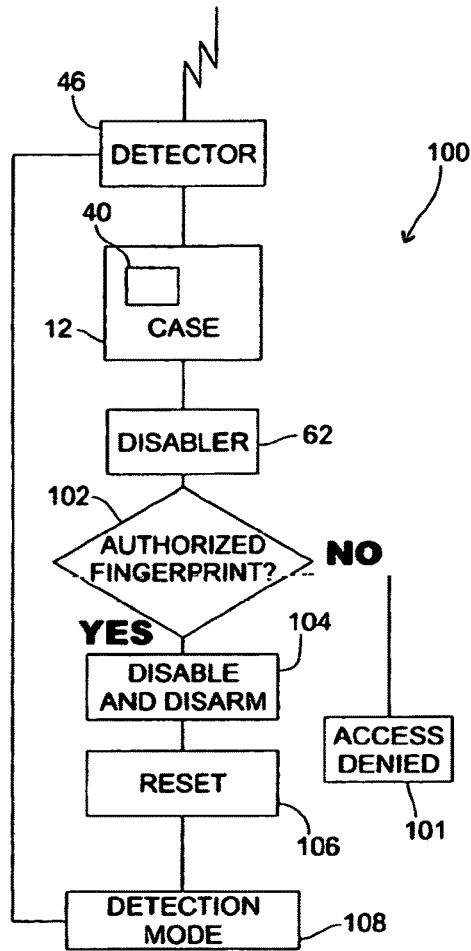
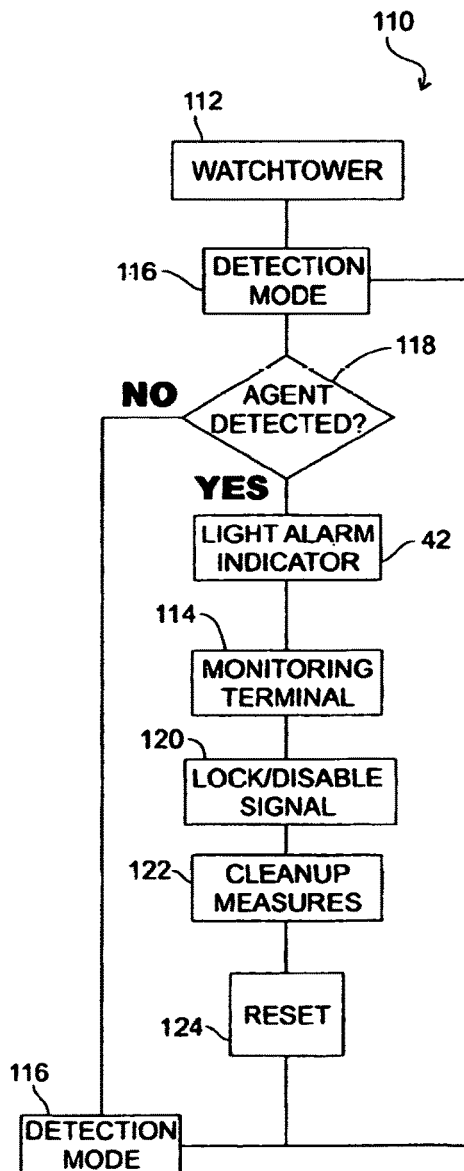


Fig. 13

**Fig. 14****Fig. 15**

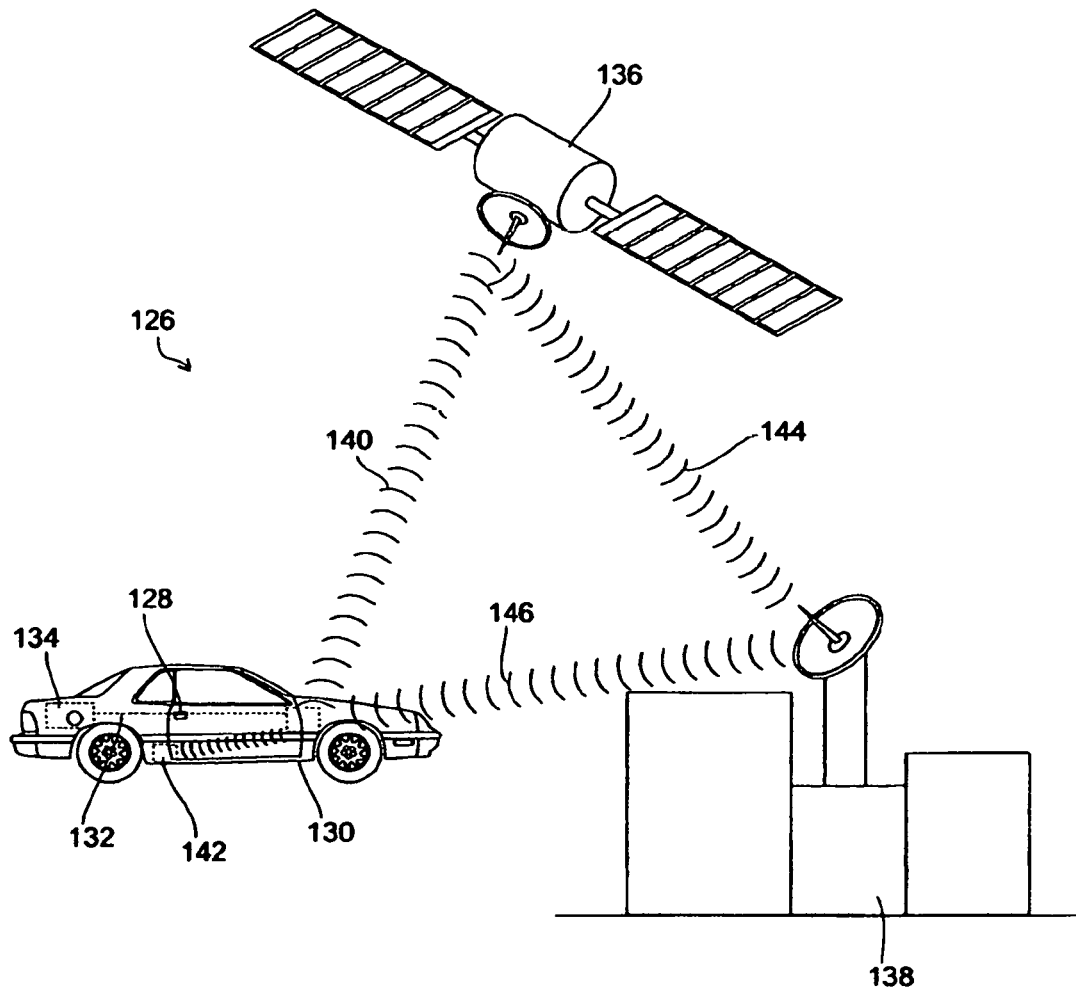
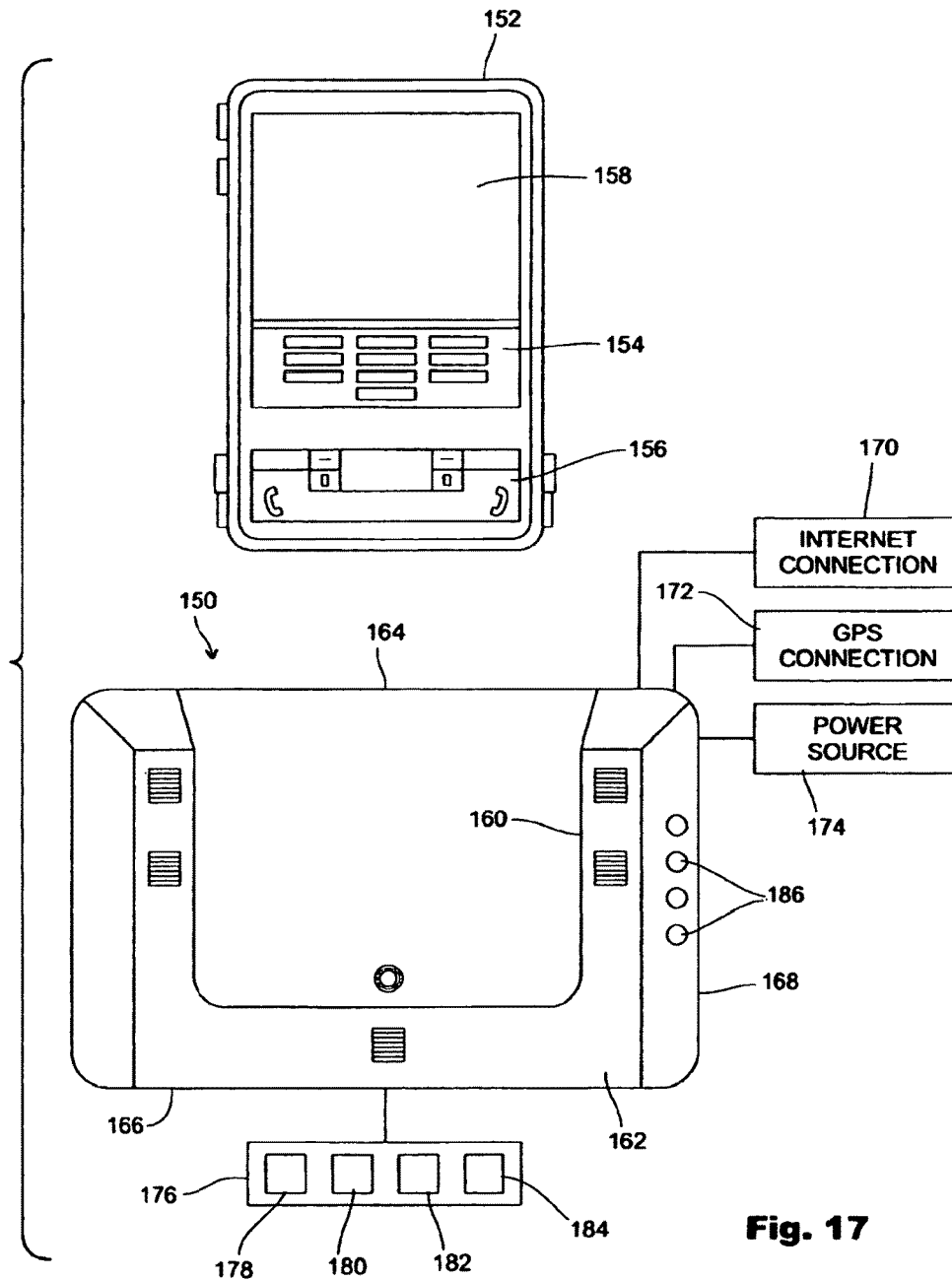


Fig. 16



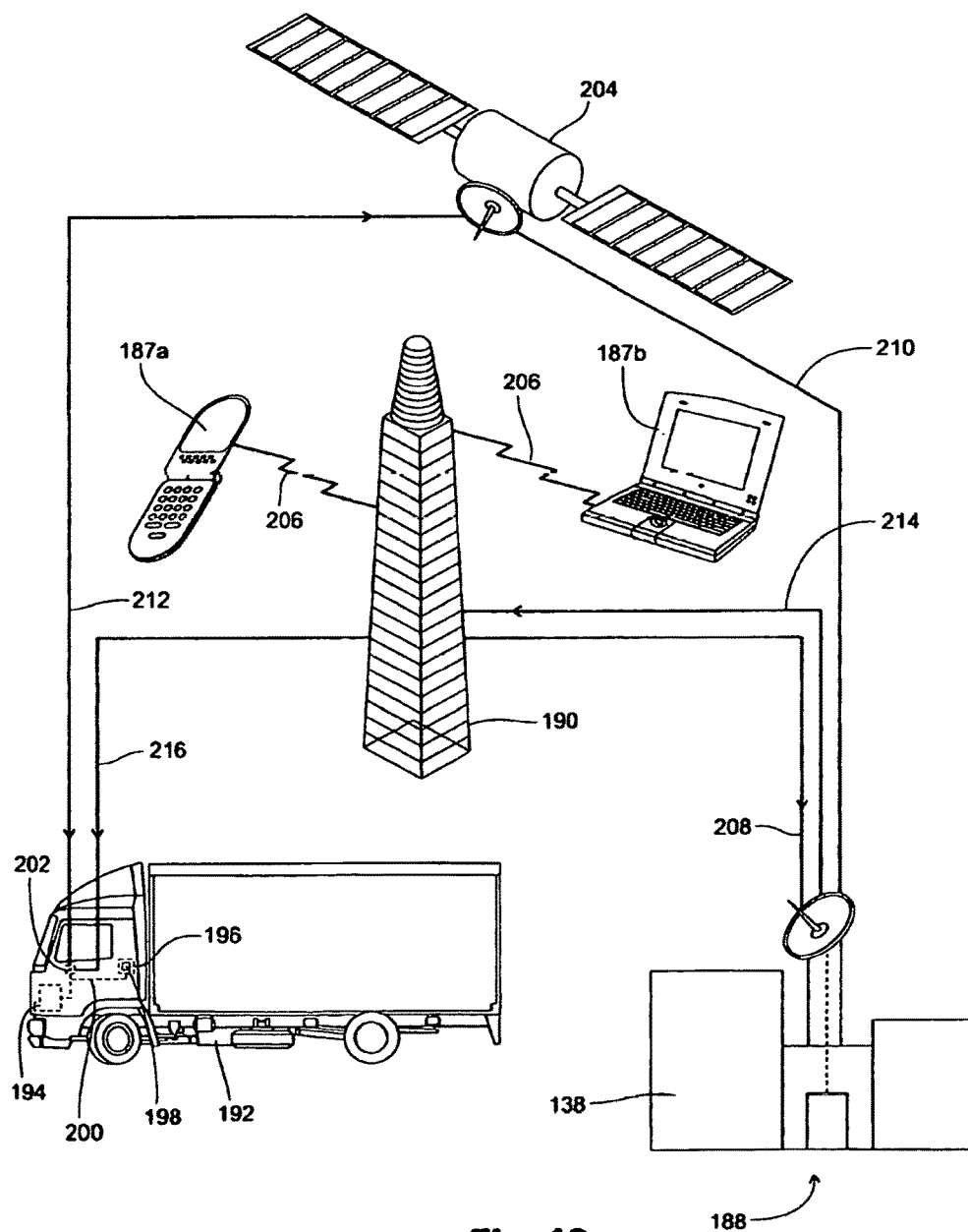
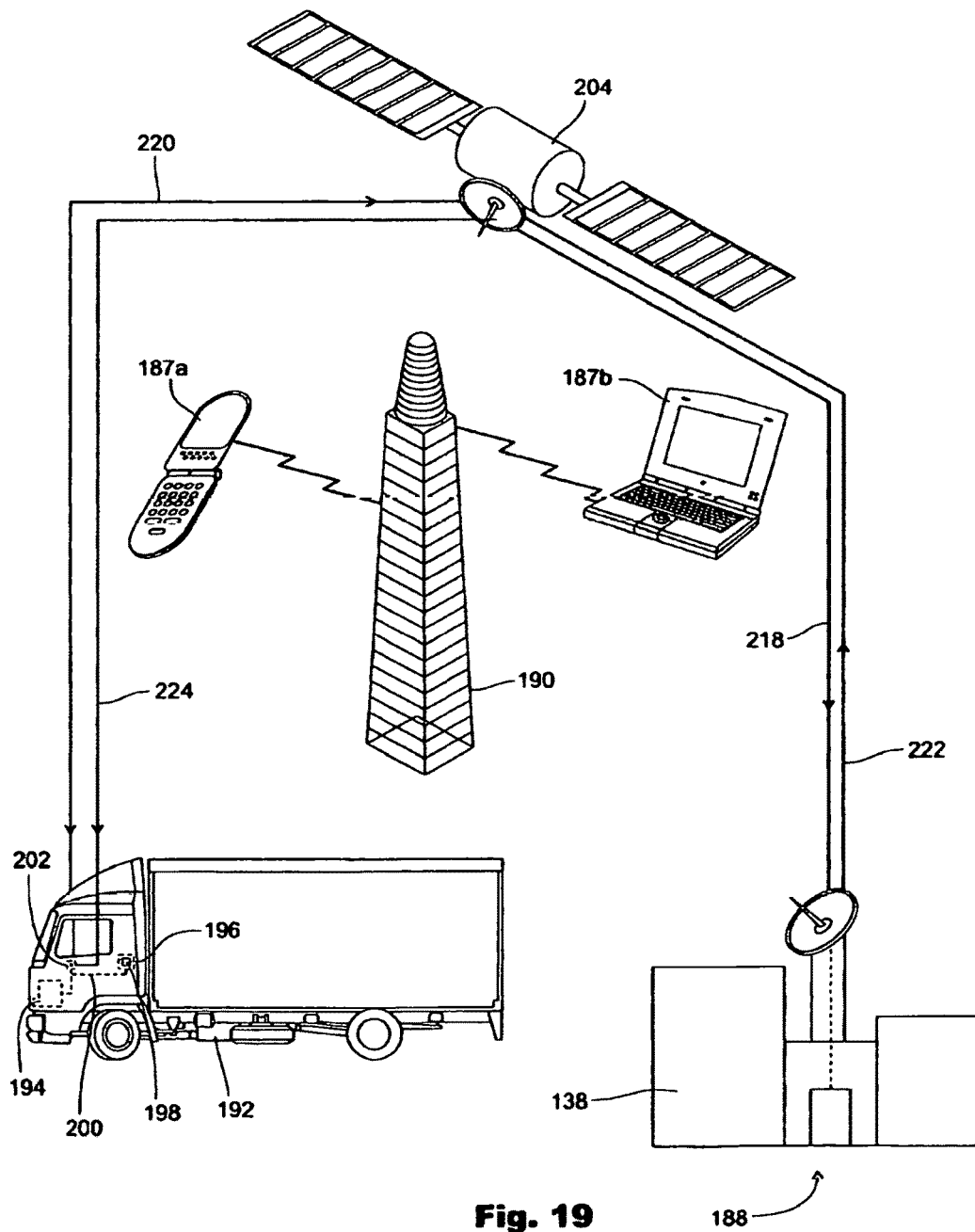


Fig. 18



US 10,163,287 B2

1

MULTI SENSOR DETECTION, STALL TO STOP AND LOCK DISABLING SYSTEM**CROSS REFERENCE TO RELATED APPLICATION**

This application is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 14/806,988 title "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Jul. 23, 2015 that issued on Mar. 7, 2017 as U.S. Pat. No. 9,589,439, the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. Pat. No. 9,589,439 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 14/021,693 title "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Sep. 9, 2013 that issued on Aug. 4, 2015 as U.S. Pat. No. 9,096,189, the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. Pat. No. 9,096,189 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 13/288,065 title "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Nov. 3, 2011 that issued on Sep. 10, 2013 as U.S. Pat. No. 8,531,280, the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. patent application Ser. No. 13/288,065 that will issue as U.S. Pat. No. 8,531,280 is a divisional application and claims the filing date and benefit of U.S. patent application Ser. No. 12/802,001 title "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on May 27, 2010, that issued on Dec. 18, 2012 as U.S. Pat. No. 8,334,761, the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. Pat. No. 8,334,761 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 12/657,356 title "Multi Sensor Detection, Stall to Stop and Lock Disabling System" filed on Jan. 20, 2010 that issued on Jan. 31, 2012 as U.S. Pat. No. 8,106,752 the entire contents of which are incorporated by reference herein in their entirety for all purposes. U.S. Pat. No. 8,106,752 is a continuation of and claims priority to U.S. Pat. No. 7,636,033. U.S. Pat. No. 7,636,033 is a continuation-in-part of and claims priority to U.S. Pat. No. 7,385,497. U.S. patent application Ser. No. 13/288,065 that will issue as U.S. Pat. No. 8,531,280 also claims the filing date and benefit of and incorporates the entire contents of U.S. patent application Ser. No. 12/657,356, now U.S. Pat. No. 8,106,752 herein by reference for all purposes. The present application also claims the filing date and benefit of and incorporates the entire contents of U.S. Pat. Nos. 9,096,189; 8,531,280; 8,334,761; 8,106,752; 7,636,033; and 7,385,497 by reference herein in their entirety for all purposes.

FIELD OF THE INVENTION

The present invention pertains to anti-terrorist detection and prevention systems, and more particularly pertains to a disabling lock mechanism combined with a chemical/biological/radiological detection system for use with products grouped together by similar characteristics in order to prevent unauthorized entry, contamination and terrorist activity.

BACKGROUND

Terrorist activity is a continuous, daily, worldwide threat to the stability, prosperity, security and peace within nations

2

and between and among nations. Its danger lies in its arbitrary destructiveness as much as in its unpredictability, and the constant threat of terrorist activity compels measures and actions that cause strain and contention in free, democratic societies as security concerns and civil liberty concerns must be balanced so that both public safety and civil liberties are maintained. Safety and security concerns can be addressed through numerous proactive steps and measures, many of which cause only minimal interference with and disruption of the daily routines of work, travel, commerce and entertainment. However, because modern industrial societies afford almost limitless places, locations, and opportunities for terrorist activities, no safety measure or security protocol will be foolproof, but many security measures, systems and protocols can be implemented that greatly minimize specific threats through fingerprint identification procedures, chemical, biological, and radiological hazard detections, bomb and explosive detection, and controlling the access to everything from shipping containers to school lockers. Thus, the prior art discloses a wide range of security measures and systems.

For example, the Fishbine et al. patent (U.S. Pat. No. 4,792,226) discloses an optical fingerprinting system that includes an optics/processor unit, a video monitor, a data terminal, and a printer for collecting and storing data characteristics of all ten individual fingerprints for printing demographic information and fingerprint images as desired on a standard booking or applicant card.

The Schiller patent (U.S. Pat. No. 4,544,267) discloses a finger identification unit that includes a fingerprint scanning apparatus using a collimated beam of light to interrogate the fingerprint of a finger placed against a platen so that successive scan positions produce signals containing fingerprint information.

The Fishbine et al. patent (U.S. Pat. No. 5,222,152) discloses a portable fingerprint scanning apparatus for optically scanning and recording fingerprint images and wirelessly transmitting such images to a mobile processing unit for verification and background checking.

The Loughheed et al. patent (U.S. Pat. No. 5,233,404) discloses an optical scanning apparatus that uses a linear charge coupled device (CCD) for recording the image of a fingerprint on the viewing surface.

The Groger et al. patent (U.S. Pat. No. 5,766,956) discloses a diode laser based sensor for undertaking optical, chemical, immunological or nucleic acid-based assay or other chemical analysis.

The Feldman patent (U.S. Pat. No. 5,938,706) discloses a multi element security system for preventing the unauthorized use of an automotive vehicle, and which includes numerous locking and control features interconnected to an onboard cpu.

The Bowker et al. patent (U.S. Pat. No. 5,963,657) discloses a safety access control for doors, handles, locks, etc., wherein the surface relief of a finger is read and verified to either allow or prevent access by the individual to the door, handle, lock, etc.

The Bonder et al. patent (U.S. Pat. No. 6,078,265) discloses a fingerprint identification security system wherein a key lock operated security system utilizes the fingerprint of the individual to control user access to the security system, such as the ignition system of an automotive vehicle.

The Anzai et al. patent (U.S. Pat. No. 6,271,745 B1) discloses a keyless authorization system for use of a motor vehicle that includes fingerprint reading units located on the exterior or interior of the motor vehicle and which are

US 10,163,287 B2

3

coupled to a control unit for scanning, comparing and matching fingerprints to allow or disallow access to the motor vehicle.

The Hwang patent (U.S. Pat. No. 6,374,652 B1) discloses a fingerprint-activated doorknob in which a detecting sensor for a fingerprint is placed on the doorknob for measuring and searching the fingerprint against previously stored fingerprint inputs to control access to the door.

The Vor Keller et al. patent (U.S. Pat. No. 6,588,635 B2) discloses a safety holster for a firearm that includes a pivotally mounted retaining member and a fingerprint sensor for scanning fingerprint information so that only authorized users can withdraw the firearm from the holster.

The Cordery et al. patent (U.S. Pat. No. 6,613,571 B2) discloses a method and system for detecting biological and chemical hazards in the mail that includes sensors placed within the mail box for sampling and testing ambient air and so that mail can be safely transported through the mail system.

The Nagata patent (U.S. Pat. No. 6,628,213 B2) discloses a coding method for digital signal coding and decoding that includes a CMI (code-marked inversion) method of signal coding.

Nonetheless, despite the ingenuity of the above devices, methods, and systems, there remains a need for a multi-detector and disabling lock system for use with various types of products collected together by common characteristics into product groupings for detecting chemical, biological and radiological agents and compounds and for selectively disabling and activating the product locks thereby preventing unauthorized entry and further contamination and preventing and thwarting terrorist activities.

SUMMARY

The present invention comprehends a chemical/biological/radiological detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping 1 include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes and lockers; while the products grouped into what may be referred to as Product grouping 2 include, but are not limited to, chemical, biological, radiological, and nuclear detectors, motion sensors and door sensors. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

The multi sensor detection and lock disabling system includes a detector case sized to fit in, upon or adjacent any of the aforescribed products for detecting harmful and dangerous chemical, biological, and radiological agents, compounds and elements. In addition, the multi sensor detection and lock disabling system is capable of transmitting a signal to lock or disable a lock on the product, and is also capable of transmitting signals to a monitoring computer terminal or PC so that appropriate defensive and safeguarding actions can be undertaken and an authorized individual can disarm and reset the locking system and the

4

multi sensor detection system. The detector case includes a power source (battery or electrical), interior compartments, Internet and GPS connections and a cpu interconnected with the Internet and GPS connections, and also interconnected with one or more off site monitoring computer terminals or PCs. The detector case includes one or more light alarm indicators that are externally visible and that light up when the chemical, biological, or radiological agent or compound is detected, and the light alarm indicators (which can be indicator lights or panels on the front of the detector case) can be color coded for denoting the specific agent or compound detected, i.e., separate and distinct colors for indicating detection of the chemical, biological, or radiological agent or compound.

The detector case is designed to hold within the interior compartments one or more interchangeable detectors, and each detector is adapted and set up to sample a specific compound or agent. Each detector includes a sound alarm, a sensor, a light alarm, and a readings panel, and is electrically interconnected (either by wire or wirelessly) to the cpu of the detector case so that information regarding the detection of the particular agent or compound can be conveyed from the detectors to the detector case cpu. Each detector can also be used as a manual, stand-alone hand held scanner.

The multi sensor detection and lock disabling system can be interconnected to a surveillance watchtower, as well as monitoring computer terminals or PCs, with the watchtower scanning shipping and cargo crates and containers being prepared for shipment or sitting for extended periods of time on a dock or at a port, at a railway site, or at an industrial storage facility. The watchtower will scan the cargo and shipping crates and containers for the light alarm indicators on detector cases that are mounted in or upon the crates and containers, and thus continuous security surveillance of the crates and containers can be maintained.

An enhanced version of the multi sensor detection and lock disabling system can be employed to prevent car and vehicle bombings. Coupling the multi sensor detection and lock disabling system with satellite service will enable the detection system to detect explosives and transmit an alert signal by satellite to monitoring equipment at a monitoring site. Upon receiving the alert signal at the monitoring site the monitoring equipment activates a stall-to-stop process for disabling the air, fuel, electrical and/or computer system of the vehicle. Moreover, upon receiving the alert signal at the monitoring site the car or vehicle will be locked by transmission of a satellite signal that disables the vehicle's electrical and ignition system thereby preventing escape of the terrorist.

It is an objective of the present invention to provide a multi sensor detection and disabling lock system for securing news racks and vending machines in order to prevent theft, unauthorized use and terrorist activity.

It is another objective of the present invention to provide a multi sensor detection and disabling lock system for preventing terrorist activity by using products grouped together by common features in several product groupings such as design similarity, similarity in the presentation of security problems and similarity with regard to the presentation of solutions to preventing terrorist solutions.

It is still yet another objective of the present invention to provide a multi sensor detection and disabling lock system that is capable of disabling an existing lock or activating a lock inside any of the products of the product grouping lists when a detector or sensor of the system is activated.

It is still yet a further objective of the present invention to provide a multi sensor detection and disabling lock system

US 10,163,287 B2

5

wherein the disabling lock system prevents the unauthorized entry, access and further contamination of the products included in the several product groupings.

A still further objective of the present invention is to provide a multi sensor detection and lock disabling system that utilizes a multi-task device for preventing terrorist activity to vulnerable products that are collected or arranged by product grouping categories.

Yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system to secure cargos and containers, especially cargo and shipping containers, against chemical, biological, radiological and nuclear terrorist activity.

Still another objective of the present invention is to provide a multi sensor detection and disabling lock system capable of detecting chemical, biological and radiological agents and compounds.

Still yet another objective of the present invention is to provide a multi sensor detection and disabling lock system that includes interchangeable detectors that operate in conjunction to detect chemical, biological and radiological agents and compounds.

Still yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system that can be implemented by business or government at a minimum cost by organizing the products to be protected into product grouping categories.

Another objective of the present invention is to provide a multi sensor detection and disabling lock system that accurately and reliably detects harmful agents, compounds and elements, and prevents the placement and storage of weapons and bombs in the range of storage containers and facilities currently available.

Still another objective of the present invention is to provide a multi sensor detection and disabling lock system wherein the interchangeable detectors that comprise part of the system can be used as stand-alone scanners.

These and other objects, features, and advantages will become apparent to those skilled in the art upon a perusal of the following detailed description read in conjunction with the accompanying drawing figures and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the primary features of the system which include a detector case, several interchangeable detectors, an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler;

FIG. 2 is a front elevational view of the multi sensor detection and lock disabling system of the present invention illustrating one of the interchangeable detectors first shown in FIG. 1;

FIG. 3a is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one lock disabler to the lock of a product, such as a container, and disengaged from the lock of the container;

FIG. 3b is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the engagement of the lock disabler to the lock of the product for locking or disabling the lock of the product so that unauthorized access is prevented;

FIG. 4 is a side elevational view of the multi sensor detection and lock disabling system of the present invention

6

illustrating the detector case mounted to the product, such as the container, with the light alarm indicators externally visible;

FIG. 5 is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of detector cases with a surveillance watchtower and a monitoring PC terminal;

FIG. 6 is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the placement of detector cases upon containers different from the containers of FIG. 5, and wherein the detectors case are interconnected to a surveillance watchtower and a monitoring PC terminal;

FIG. 7 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one automatic/mechanical lock disabler to the lock of a standalone news rack;

FIG. 8 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating one interchangeable detector placed within the stand-alone news rack;

FIG. 9 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case having color coded front panels for specifically indicating the agents, compounds or elements that have been detected;

FIG. 10 is a rear elevational view of the multi sensor detection and lock disabling system of the present invention illustrating the GPS, Internet and power source connections;

FIG. 11 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector with the detector case and the steps undertaken by the system when an agent or compound is detected;

FIG. 12 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the sequence of steps undertaken by one detector when functioning as a stand alone scanner for detecting an agent or compound;

FIG. 13 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector case with the automatic/mechanical lock disabler for activating the lock disabler upon detection by the system of an agent or compound;

FIG. 14 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating interconnection of the detector case with the fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public upon detection of the agent or compound;

FIG. 15 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the system with a surveillance watchtower and a monitoring PC or computer terminal for monitoring containers, such as shipping or cargo containers, that may sit for extended time periods on docks, at rail yards, and at industrial storage facilities;

FIG. 16 is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the integration of the detection system with a satellite and monitoring equipment at a monitoring site for detecting explosives placed in a vehicle and then transmitting signals to the satellite and then to the monitoring site for disabling and locking the vehicle;

US 10,163,287 B2

7

FIG. 17 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the features and elements of the detector case to a cell phone and cell phone case;

FIG. 18 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of a GPS satellite, a monitoring site and a cell phone tower for communicating to and with an electronic device such as a laptop computer or a cell phone for transmitting signals to a vehicle for activating an onboard stall-to-stop device for bringing the vehicle to a halt; and

FIG. 19 is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the use of a GPS satellite in conjunction with the monitoring site and monitoring equipment to relay commands and signals to the cpu or transceiver of the vehicle for stopping or locking the vehicle in response to a signal that a certain type of event (detection of a bomb, engine failure or malfunction or unauthorized use) has occurred or is in process.

DETAILED DESCRIPTION OF REPRESENTATIVE EMBODIMENTS

Illustrated in FIGS. 1-19 is a multi sensor detection and lock disabling system 10 for preventing terrorist activity by monitoring, detecting, and securing those critical areas; sites, and facilities vulnerable to terrorist activity. The first step is the identification of critical areas, sites, locations and facilities that are vulnerable to terrorist activity as convenient places to store and plant explosives and bombs and spread biological, chemical or radiological agents and compounds, followed by the disposition of the multi sensor detection and lock disabling system 10 for monitoring, detecting, and securing the particular location or site. Vulnerable sites, locations, facilities and areas are nearly limitless in their variety; in order to categorize the protection the present invention provides an anti-terrorist product grouping strategy has been developed wherein products made from the same or similar material, products having the same or similar design, and products presenting the same or similar security problems are grouped together with the multi sensor detection and lock disabling system 10 for preventing terrorist activity. For example, two preferred product groupings can be Product Grouping I: cargo containers, shipping containers, cargo planes, freight train cars, tractor trailers, mail carriers (UPS, FedEx), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans and utility vehicles. Product Grouping II: chemical detectors, biological detectors, radiological detectors, nuclear detectors, motion sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems. In addition to grouping products together by features, designs and materials, the multi sensor detection system 10 includes a lock disabling capability for disabling an existing lock or activating a lock on or inside any of the aforementioned products when a detector or sensor of the system is activated. The lock disabling feature is a crucial component of the invention in so far as it prevents unauthorized, unequipped or untrained individuals from gaining access and entry to the site and causing further contamination of the site.

8

As shown in FIGS. 1-10, the multi sensor detection and lock disabling system 10 includes at least one—and preferably many—detector case 12 that can be placed in, on, upon or adjacent the product, such as the shipping containers 14 of FIGS. 4 and 5 resting upon a platform 16 or the cargo container 18 of FIG. 6 sitting upon a seaport dock or pier 20. The detector case 12 includes a top 22, a bottom 24, a pair of opposed sides 26 and a front side or panel 28 and an opposite rear or back side 30. The rear side 30 has connections or contacts that can include an Internet connection 32, a GPS connection 34 and a power connection 36 for a power source. The power source for the detector system 10 can be any conventional battery or electrical source. The detector case 12 includes an interior chamber divided into a number of compartments 38 for holding therein agent or compound detection means hereinafter further described. A cpu 40 is mounted within the detector case 12 and electrically interconnects, routes, and transmits signals among items hereinafter further described and also communicates with a monitoring site and monitoring equipment. The front side 28 of the detector case 12 includes indicator means for visually indicating that a specific agent, compound or element has been detected. The indicator means can include color coded indicator lights 42 in panel form, as shown in FIG. 9, with each indicator light panel 42 lighting up with a specific color corresponding to the detection of a specific agent or compound; or color coded indicator lights 44, as shown FIG. 1, that correspond to and individually light up on the detection of a specific agent or compound (chemical, biological, or radiological).

As shown in FIGS. 1, 2 and 9-13, the multi sensor detection and lock disabling system 10 includes a plurality of detectors 46 with each detector 46 adapted for and set up to sample for a specific agent or compound (biological, chemical, or radiological); and the detectors 46 are interchangeable for adapting to the needs and demands of future technology. The detectors 46 can also be used as stand alone scanners. In the preferred embodiment of the invention, at least three detectors 46 are placed within the detector case 12 with one detector 46 for specifically sampling biological agents or compounds, one detector 46 for sampling chemical agents or compounds, and one detector 46 for sampling radiological agents or compounds. The detectors 46 are interconnected to the cpu 40 of the detection system 10 by conventional connections that can be wire or wireless for transmitting the appropriate signals to the cpu 40 upon detection of the particular agent or compound. As shown in FIG. 2, each detector 46 includes on its front plate or facing surface a sound alarm indicator 48, a readings panel 50 comprising a plastic shield and LED lights for displaying the various read-out messages, a sensor 52 for detecting the specific agent, element or compound, and a light alarm indicator 54 that can be color coded for each specific agent and which is externally visible when the detector 46 is used as a stand alone scanner. Each detector 46 includes a conventional microprocessor for controlling the various functions and generating the appropriate signals for transmission to the cpu 40 of the detector case 12.

As shown in FIGS. 1, 3a, 3b, 9, and 13-15, used in conjunction with the multi sensor detection and lock disabling system 10 is at least one automatic/mechanical lock disabler 56—and depending upon the number of products being monitored there can be one lock disabler 56 for each product. The automatic/mechanical lock disabler 56 is physically connected to the detector case 12 by a wire or cable 58 for receiving signals therefrom for disabling an existing lock or activating a lock inside a product to prevent

US 10,163,287 B2

9

access to the product. By way of example, FIG. 3a shows the automatic/mechanical lock disabler 56 mounted—by any conventional means—to the lock 60 of the shipping container 14 shown in FIGS. 4 and 5 and connected by wire 58 to the cpu 40 of the detector case 12. The lock disabler 56 is in the non-activated or disengaged state in FIG. 3a. FIG. 3b shows the automatic/mechanical lock disabler 56 mounted to the lock 60 of the shipping container 14 and in the activated or engaged state after detection of an agent or compound by the system 10 thereby for locking or disabling the lock 60 of the shipping container 14 and preventing unauthorized entry and access by unauthorized, untrained and unequipped individuals. In FIGS. 3a and 3b the lock 60 secures doors of the shipping container 14 that can be slidably or pivotably opened and closed.

In addition to the automatic/mechanical lock disabler 56, the multi sensor detection and lock disabling system 10 can also utilize a fingerprint biometric lock with disabler 62 as shown in FIGS. 1 and 14. The fingerprint biometric lock with disabler 62 is interconnected to the cpu 40 of the detector case 12 for receiving transmissions therefrom after detection of an agent or compound has occurred so that the lock on the product can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler 62 occurs when the fingerprint of the individual is placed on the fingerprint-matching pad 64, and if a match occurs with a known fingerprint stored by the cpu 40, then the individual can reset the fingerprint biometric lock with disabler 56 by turning the manual lock disabler 66. The fingerprint biometric lock with disabler 62 is mounted to the lock of the product in a manner similar to the mounting of the automatic/mechanical lock disabler 56 that is shown in FIGS. 3 and 3b.

FIGS. 4 and 5 show one manner of disposition or placement of the detector case 12 in relation to the product, i.e., the shipping container 14, with the color coded indicator lights 42 externally viewable; FIG. 5 shows a number of shipping containers 14 each equipped with a detector case 12 and integrated with elements hereinafter further described for continuously monitoring the shipping containers 14 as they sit for an extended period of time on the truck or rail platform 16. FIG. 6 illustrates several cargo containers 18 sitting on the shipping dock or pier 20, with each cargo container 18 having a detector case 12 mounted thereon and integrated with and monitored by elements shown in FIG. 5 and hereinafter further described.

FIG. 7 illustrates a typical product from product grouping 1 that is monitored by the multi sensor detection and lock disabling system 10 of the present invention; specifically, FIG. 7 shows a news rack 68 with one automatic/mechanical lock disabler 56 mounted to and interconnected with the locking mechanism of the news rack 68. As long as there is no detection of any agent or compound, the lock disabler 56 is in the disengaged state, and the individual can deposit the coin amount in the chute and then freely open the glass panel 70 by the handle 72 for removing a paper. However, the lock disabler 56 would be activated upon detection of the harmful agent or compound and receipt of a signal from the cpu 40 for locking or disabling the locking mechanism thereby denying access to the interior of the news rack 68 from all untrained, unauthorized and unequipped individuals.

FIG. 8 illustrates one detector 46 disposed within the news rack 68 and which is visible through the panel 70 for detecting one specific agent, compound or element. The detector 46 functions as a stand-alone scanner and can be wirelessly interconnected to off site monitoring equipment.

10

FIG. 11 illustrates a representative schematic 74 for describing the signal transmission process from the detector 46 to the cpu 40 of the detector case 12. The external stimulus 76 would be the chemical, biological or radiological agent or compound. If there is no detection of the agent or compound, the detector 46 will stay in the sensing mode 78. However, detection of the specific agent will trigger the sound alarm 80 and the light alarm 82, and instant transmittal of a signal to the cpu 40. The readings 84 can be stored by the cpu 40 for verification and future review and evaluation. After all the appropriate corrective and preventative measures have been undertaken by the trained and authorized personal, and the site has been cleansed of the contamination, authorized and equipped personal can then reset the system 10.

FIG. 12 illustrates a representative schematic 88 for the detector 46 when used as stand-alone scanner. The detector 46 undergoes the same essential steps as illustrated in FIG. 11, with the exception of the signal transmission to the cpu 40. The detector 46 remains in detection mode 78 until an agent is detected, and then the various functions—light alarm 82, sound alarm 80, storage of readings 84, and, after the appropriate security and safety steps have been carried out by authorized personal, detector reset 90 by authorized personal can occur thereby placing the detector 46 back in detection or sensing mode 78.

FIG. 13 is a representative schematic 92 that illustrates the steps undertaken by the system 10 to lock or disable a lock, such as the lock 60 for the shipping container 14 shown in FIGS. 3a and 3b. Upon detection of the agent (chemical, biological, radiological) the alarm light indicators 42 or 44 will light up providing external indication that an agent has been detected. In addition, the system 10—the cpu 40—will transmit a lock/disable lock signal 94 to the automatic/mechanical lock disabler 56 to lock or disable the lock on the product, such as the lock 60 on the shipping container 14 of FIGS. 3a-5. This prevents unauthorized, unequipped, or untrained individuals from entering or gaining access to the product for which a dangerous and perhaps lethal agent has been detected. After the proper authorities and authorized personal have been notified and all the appropriate security, preventative and clean up measures have been undertaken, the authorized individual can perform the disarm and reset function 96 for the system 10 placing the system 10 back in the detection mode 98.

FIG. 14 is a representative schematic 100 illustrating the use of the fingerprint biometric lock with disabler 62 with the system 10. Upon detection of the agent or compound by the detector, the various alarms would sound and light up (shown in previous figures), and the cpu 40 would then transmit a signal to the fingerprint biometric lock with disabler 62 to lock or disable the lock on the product, such as the lock 60 on the shipping containers 14 shown in FIGS. 3a-5. The shipping containers 60 would remain locked and in an access denied mode 101 should an attempt be made to gain access to the container 60 by opening the lock 60 with an unauthorized fingerprint. However, a fingerprint that matches stored and authorized fingerprints 102 would indicate an authorized individual, and would allow the individual to disable and disarm 104 the lock 60 of the shipping container 14. The fingerprint biometric lock with disabler 62 would then be reset 106 after the appropriate safety, cleanup, and protection measures are completed, and the system 10 would be reset and placed back in the detection mode 108.

FIG. 15 is a schematic representation 110 that illustrates the integration of a surveillance watchtower 112 and a monitoring terminal or PC 114 for monitoring products such

US 10,163,287 B2

11

as the shipping containers 14 or cargo containers 16 that sit for extended periods of time of docks, piers 20, truck terminals, rail yards, shipping platforms 16 and industrial sites as shown in FIGS. 5 and 6. The watchtower 112 would maintain continuous surveillance over a number of shipping containers 60, for example, with detector cases 12 mounted in or on each container 14 and set in detection mode 116 with one or more detectors 46 disposed in each detector case 12. The watchtower 112 would continuously scan for light alarm indicators 42 and 44 on the products, such as the containers 14 or 18, and the watchtower 112 would be interconnected and integrated with the monitoring terminal or PC 114. Upon detection 118 of an agent or compound in one or more of the shipping containers 14, the appropriate light alarm indicators 42 or 44 would light providing visible confirmation of the detection of the specific agent or compound. The cpu 40 would transmit a lock/disable signal 120 to the lock 60 on each respective shipping container 14 to lock or disable the lock 60 thus preventing access to that respective shipping container 14. In addition, signal transmissions would be sent to the monitoring terminal or PC 114 (which could be off site) thereby alerting authorized security personnel of the contamination event. With the information received at the monitoring terminal 114, authorized personnel would then be notified and dispatched to the area to undertake the appropriate safety and cleanup measures 122. Such measures would also include disarming the lock disabling system in order to gain access to the shipping container 14. After all the cleanup and security measures are completed by the trained and properly equipped authorities, the detection system and the lock disabling feature would reset 124 and the detection system would again be placed in detection mode 116.

FIG. 16 is a schematic representation 126 that illustrates an enhanced version of the multi sensor detection and lock disabling system 10 for preventing car and vehicle attacks and bombings. The lock disabling system 10 would be interconnected to the locking system and mechanism 128 of the vehicle 130. In addition, a stall to stop disabling link 132 can be made with the fuel, air, and electrical system 134 of the vehicle 130. The enhanced version incorporates a satellite 136 for signal receipt and transmission from the vehicle 130 in which the detector system 10 is placed to a monitoring site and monitoring equipment 138. As shown in FIG. 16, a detection signal 140 would be sent to the satellite 136 by the detection system 10 upon detection of a bomb or explosive 142 hidden in the vehicle 130. The satellite 136 would then transmit an alert signal 144 to the monitoring site 138 with the signal 144 containing the relevant data to evaluate the nature of the threat. The monitoring site 138 would then transmit a stall to stop signal 146 to the detection system 10 to lock the vehicle 130 and/or disable the electrical system of the vehicle 130 thereby disabling the vehicle 130, preventing access to the vehicle 130 by locking the vehicle 130, and preventing any terrorist in the vehicle 130 from escaping.

The detector case 12 can be modified and adapted for inclusion with cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, suitcases; and briefcases. In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring.

The system 10 and the watchtower 112, along with the satellite 136 and the monitoring site 138 can be adapted or incorporated with cell phone towers and satellites for use

12

with satellite communication and/or a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency inter-connected to a central processing unit (cpu), such as cpu 40, or a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween. The aforementioned telecommunication and radio communication means can be interactive with any type of motive vehicle that includes but is not limited to cars, trucks, vans, SUVs, trains, subways, boats, ships and airplanes, and which is reported stolen, experiences a loss of brakes, or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted to the vehicle and which detection causes an automatic signal transmission or a signal transmission is activated when a call is made to the monitoring station by an authorized person. The authorized individual includes but is not limited to the owner, pilot, conductor, captain, police highway patrol, security guard and military personnel to the monitoring equipment for activating a vehicle slowdown or stall-to-stop disabling system that similar to the disabling system 126 shown in FIG. 16, or incorporating features of the system 126 shown in FIG. 16, from the monitoring equipment to the vehicle. The activation of the stall-to-stop disabling means or the vehicle slowdown disables or engages the computer, electrical, fuel and air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to the brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.

In addition, the basic stall-to-stop disabling means or the vehicle slowdown means and device can be adapted, modified or designed to include: an open bust or open platform for integrating any new and innovative technology; warning lights indicators; sound alarm indicators; voice alarm indicators; a cell phone to transmit to the vehicle a signal for slowing and halting the vehicle; and a lock disabling system or means to lock a thief or terrorist inside the vehicle after a transmission is received or sent. Open bust or open platform also refers to the compatibility of the detector case 12, or the incorporation of its features in cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, briefcases, and suitcases, etc., with other communication, transmission and surveillance systems whereupon the detector case 12, and its features, can be seamlessly integrated with other new and emerging systems and technologies.

Thus, as shown more specifically in FIG. 17, by way of a representative example the features and elements of the detector case 12 are shown as being incorporated into cell phone detector case 150 and associated cell phone monitor 152. The cell phone monitor 152 includes the standard keypad functions 154 and more specialized system use (ring tone, email, photos, texting) functions 156 as well as a viewing screen 158. The cell phone detector case 150 includes a recharging cradle or seat 160, a front side 162, a top 164, a bottom 166, and a pair of opposed sides 168. At the back of the cell phone detector case 150 are connections, contacts, and ports for at least an Internet connection 170, a GPS connection 172, and a contact, plug, or port for a power source 174. The power source for the cell phone detector case 150 can be any conventional rechargeable battery source or standard electrical power from a standard electrical receptacle or outlet.

As shown in FIG. 17, the cell phone detector case 150 includes one or more sensor/detector units, cells, or com-

US 10,163,287 B2

13

ponents 176 built into and incorporated into the case 150. The detector 176 includes generally disposed at the front 162 of the case 150 the following types of indicators: a sound alarm indicator 178, a readings panel 180, a sensor 182 for detecting one or more specific types of agents, elements, chemicals, compounds, etc., and a light alarm indicator 184. The sensor/detector 176 will be interconnected to the power source 174. In addition, mounted on and externally visible on the sides 168 or front 162 of the case 150 are a plurality of color coded indicator lights 186 with each light 186 corresponding to a specific agent, element, chemical, compound, etc., and lighting up when that agent is detected by the sensor/detector 176. The color coded indicator lights 186 will be electrically interconnected to the sensor/detectors 176 via any standard microprocessor. The cell phone detector case 150 and cell phone monitor 152 thus comprise a hand-held, easily portable and transportable detection means that is both effective and unobtrusive in its disposition and use.

FIGS. 18 and 19 illustrate representative examples of the integration of portable electronic communication or telecommunication devices such as a cell phone 187a and/or a laptop computer 187b with the monitoring equipment 138 located at a predesignated monitoring site 188, and operating in conjunction with either a satellite and/or a cell phone tower 190 to transmit and receive signals and commands among each other and to a vehicle 192, such as a truck, as part of a stall-to-stop disabling system for slowing and stopping the vehicle 192 and locking a thief, terrorist, or unauthorized individual in the vehicle 192 if needed. A wide range of events can trigger and initiate the stall-to-stop system and the locking or lock disabling system and mechanism, and the event doesn't have to be limited to the detection of a bomb or a chemical, biological, or radiological agent, element, or compound. The events can include, but is not limited to, detection of an engine problem to engine failure to the unauthorized use (stealing) of the vehicle 192. The vehicle 192 includes an electromotive system 194 that comprises, among other components, an onboard computer(s), electrical, fuel and air systems, as well as brakes, ignition, steering, and transmission. Also integrated with and capable of communicating with the vehicle's 192 electromotive system 194 is a stall-to-stop system while a lock disabling mechanism 196 is able to engage and disengage or disable the vehicle's 192 locking mechanism 198 upon receipt of the appropriate commands via a lock disabling communication channel or link 200. This link 200 can also accommodate the stall-to-stop system commands and signals, and thus is a multi-channel communication link. A CPU or a transceiver 202 is programmed to receive signals from the cell phone tower 190 and/or to a GPS satellite 204 and is interconnected with the stall-to-stop system and the lock disabling system 196 via link 200 for engaging the electromotive system 194 and actuating the lock disabling system 196 to stop the vehicle 192 and lock inside the vehicle 192 anyone such as a thief, terrorist or other unauthorized individual.

A representative example for stopping, disabling, and locking the vehicle 192 that utilizes the cell phone tower 190 wherein the activation and/or distress signal 206 originates from the cell phone 187a or the laptop 187b and such activation signal 206 travels to the cell phone tower 190 that is nearest the current location of the vehicle 192. A signal 208 is then transmitted to the monitoring site 188 and specific monitoring equipment 138 that can also include but is not limited to cell phones, laptops, desktop PC's, notebook PC's and LCD monitors. The monitoring site 138 then

14

communicates by signal 210 to the GPS satellite 204 that an original or activation signal has been received and then the GPS satellite 204 locates and communicates by multiplex signal 212 with the CPU or transceiver 202 on the vehicle 192 and exchanges information on the type of problem, situation, location, and vehicle speed. The monitoring equipment 138 then transmits a signal 214 to the cell phone tower 190 that communicates with the transceiver 202 and/or CPU of the vehicle 192 to initiate or execute any commands that will actuate the stall-to-stop disabling link 200 and lock disabling system 196 for bringing the vehicle 192 to a halt and actuating the vehicle's 192 locking mechanism 198 for locking the thief, terrorist, or other unauthorized person inside the vehicle 192 if needed.

FIG. 19 illustrates a representative example wherein the stall-to-stop system and the lock disabling system 196 are utilized in conjunction with the GPS satellite 204. In FIG. 19 a signal has traveled to the satellites nearest the vehicle's 192 current location and then the signal 218 has traveled to the monitoring equipment 138 and monitoring site 188 which can include but is not limited to satellite cell phones, satellite monitors, cell phones, laptops, desktop PC's, notebook PC's, and LCD monitors. The GPS satellite 204 then locates and communicates with the CPU and/or transceiver 202 on the vehicle 192 via a multiplex (two-way) signal 220 in order to exchange information on such distress and danger event parameters as the specific problem situation, location, and vehicle speed. The monitoring equipment 138 then transmits a signal 222 back to the GPS satellite 204 that in turn communicates via another signal 224 with the CPU and/or transceiver 202 to execute any commands to the stall-to-stop system for executing the disengagement of the vehicle's 192 electromotive system 194 for bringing the vehicle 192 to a halt and for actuating the lock disabling system 196 to direct the lock disabling link 200 to actuate the locking mechanism 198 thereby locking the vehicle 192 and anyone inside the vehicle 192.

The present invention comprehends a chemical/biological/radiological/nuclear/explosive/human/contraband detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars, United Parcel Services™ (UPS™), Federal Express™ (FedEx™), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans, unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), and utility vehicles; the products grouped into what may be referred to as Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, door sensors, speed sensors, biometric sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems, detection of humans, detection of contraband, temperature, and shock levels; the products grouped into what may be referred to as Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases,

US 10,163,287 B2

15

PDA cases, carry-on cases, suitcases, eyeglass, briefcases, detector cases of locks, detector cases of tags, detector cases that is mounted to, detector cases that is affixed to, detector cases that is outside of, detector cases that is inside of, and detector cases that is adjacent to; the products grouped into what may be referred to as Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless communication devices, monitoring sites, monitoring terminals, web servers, desktop personal computers (PCs), notebook personal computers (PCs), laptops, satellite cell phones, cell phones, Universal Mobile Telecommunications System (UMTS) phones, personal digital assistants (PDAs), liquid crystal display (LCD) monitors, and satellite monitoring, remote control key fobs, two-way communication key fobs, handhelds; the products grouped into what may be referred to as Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Wi-Max, Internet, Ethernet, Broadband, Network Bandwidth, Wireless, Wired, Text Messaging, Cellular, Satellite, Telematics, Wide Area Network (WAN), Wireless Wide Area Network (WWAN), Local Area Network (LAN), Radio Frequency (RF), Broadband Wireless Access (BWA), Global Positioning System (GPS), General Packet Radio Services (GPRS), Global System for Mobile (GSM), Wideband Code Division Multiple Access (W-CDMA), Universal Mobile Telecommunications System (UMTS), Short Message Service (SMS); the products grouped into what may be referred to as Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature. The products grouped into what may be referred to as Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside or outside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

While the invention has been shown and described in a preferred embodiment, it will be apparent to those skilled in the art that numerous alterations, modifications, and variations will possible and practicable without departing from the spirit and scope of the invention as set forth by the appended claims.

What is claimed:

1. Monitoring equipment that is at least one of products grouped together by common features of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone interconnected to a lock for communication therebetween; the monitoring equipment comprising:

at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between the monitoring equipment and the lock;

16

a transmitter for transmitting signals and messages to at least one of a remote lock, an electrical lock, a mechanical lock, or automatic lock;

a receiver for receiving signals from at least one of a remote lock, an electrical lock, a mechanical lock, or automatic lock;

a lock disabling mechanism that is able to engage (lock), or disengage (unlock), or disable (make unavailable) the monitoring equipment after a specific number of tries;

a short-range radio frequency (RF) connection that is near-field communication (NFC);

at least one of the satellite connection, Bluetooth connection, WiFi connection, Internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection that is capable of signal communication with the transmitter or the receiver,

at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature recognition system; and

the monitoring equipment being capable of sending signals to engage (lock), disengage (unlock), or disable (make unavailable) at least one of a remote lock, an electrical lock, a mechanical lock, or automatic lock, whereupon a signal is sent to the receiver of the monitoring equipment from at least one of the remote lock, electrical lock, mechanical lock, or automatic lock, the signal comprising at least one of location data or lock status data to be sent to the monitoring equipment.

2. Monitoring equipment that is at least one of products grouped together by common features of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone interconnected to at least one of a home lock, a building lock, or a cargo container lock for communication therebetween; the monitoring equipment comprising:

at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between the monitoring equipment and the lock;

a transmitter for transmitting signals and messages to at least one of a home lock, a building lock, or a cargo container lock;

a receiver for receiving signals from at least one of a home lock, a building lock, or a cargo container lock;

a lock disabling mechanism that is able to engage (lock), or disengage (unlock), or disable (make unavailable) the monitoring equipment after a specific number of tries;

a short-range radio frequency (RE) connection that is near-field communication (NFC);

at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RE) connection, or GPS connection that is capable of signal communication with the transmitter or the receiver;

at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature recognition system; and

the monitoring equipment being capable of sending signals to engage (lock), disengage (unlock), or disable (make unavailable) at least one of a home lock, a building lock, or a cargo container lock whereupon a

US 10,163,287 B2

17

signal is sent to the receiver of the monitoring equipment from at least one of the home lock, building lock, or cargo container lock, the signal comprising at least one of location data or lock status data to be sent to the monitoring equipment.

3. Monitoring equipment that is at least one of products grouped together by common features of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal, digital assistant (PDA) or smart phone interconnected to a vehicle lock for communication therebetween; the monitoring equipment comprising:
 - at least one of a central processing unit (CPU), a network processor, or a front end processor for communication between the monitoring equipment and the lock;
 - a transmitter for transmitting signals and messages to at least one of a manned or unmanned aerial vehicle lock, a manned or unmanned ground vehicle lock, or a manned or unmanned sea vehicle lock;
 - a receiver for receiving signals from at least one of a manned or unmanned aerial vehicle lock, a manned or unmanned ground vehicle lock, or a manned or unmanned sea vehicle lock;
 - a lock disabling mechanism that is able to engage (lock), or disengage (unlock), or disable (make unavailable) the monitoring equipment after a specific number of tries;
 - a short-range radio frequency (RF) connection that is near-field communication (NFC);
 - at least one of the satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection that is capable of signal communication with the transmitter or the receiver;
 - at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature recognition system; and
 - the monitoring equipment being capable of sending signals to engage (lock), disengage (unlock), or disable (make unavailable) at least one of a manned or unmanned aerial vehicle lock, a manned or unmanned ground vehicle lock, or a manned or unmanned sea vehicle lock, whereupon a signal is sent to the receiver of the monitoring equipment from at least one of the manned or unmanned aerial vehicle lock, manned or unmanned ground vehicle lock, or manned or unmanned sea vehicle lock, the signal comprising at least one of location data or lock status data to be sent to the monitoring equipment.
4. A communication device comprising:
 - at least one central processing unit (CPU);
 - at least one motion sensor in communication with the at least one CPU;
 - at least one viewing screen for monitoring in communication with the at least one CPU;
 - at least one global positioning system (GPS) connection in communication with the at least one CPU;
 - at least one of an internet connection Wi-Fi connection in communication with the at least one CPU;
 - at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;
 - at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication

18

device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;

- at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;
 - at least one biometric sensor in communication with the at least one CPU for providing biometric authentication to access the communication device;
 - at least one or more detectors in communication with the at least one CPU for detecting at least one of a chemical, biological, radiological, or explosive agents;
 - at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and
 - at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or send signals to detect at least one of a chemical biological, radiological, or explosive agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.
5. A monitoring device, comprising:
 - at least one central processing unit (CPU);
 - at least one temperature sensor in communication with the at least one CPU for monitoring temperature;
 - at least one motion sensor in communication with the at least one CPU;
 - at least one viewing screen for monitoring in communication with the at least one CPU;
 - at least one global positioning system (GPS) connection in communication with the at least one CPU;
 - at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;
 - at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;
 - at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;
 - at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;
 - at least one biometric sensor in communication with the at least one CPU for providing biometric authentication to access the communication device;
 - at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;
 - one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;
 - at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and
 - at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or send signals to

US 10,163,287 B2

19

detect at least one of a chemical biological, radiological, or explosive agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.

6. A monitoring equipment, comprising:

- at least one central processing unit (CPU);
- at least one motion sensor in communication with the at least one CPU;
- at least one light indicator in communication with the at least one CPU;
- at least one viewing screen for monitoring in communication with the at least one CPU;
- at least one global positioning system (GPS) connection in communication with the at least one CPU;
- at least one of an internet connection Wi-Fi connection in communication with the at least one CPU;
- at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;
- at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;

20

- at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;
- at least one biometric sensor in communication with the at least one CPU for providing biometric authentication to access the communication device;
- at least one or more detectors in communication with the at least one CPU for detecting at least one of a chemical, biological, radiological, or explosive agents;
- at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and
- at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or send signals to detect at least one of a chemical biological, radiological, or explosive agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.

* * * * *

APPEAL,CLOSED,PRO SE

**US Court of Federal Claims
United States Court of Federal Claims (COFC)
CIVIL DOCKET FOR CASE #: 1:23-cv-00811-EGB**

GOLDEN v. USA
Assigned to: Senior Judge Eric G. Bruggink
Demand: \$1,000,000
Case in other court: 24-02256
Cause: 28:1491 Tucker Act

Date Filed: 05/31/2023
Date Terminated: 04/24/2024
Jury Demand: None
Nature of Suit: 508 Patent
Jurisdiction: U.S. Government Defendant

Plaintiff**LARRY GOLDEN**

represented by **LARRY GOLDEN**
740 Woodruff Road
#1102
Greenville, SC 29607
(864) 288-5605
PRO SE

V.

Defendant**USA**

represented by **Grant Drews Johnson**
DOJ-Civ
1100 L Street NW
Suite 8002
Washington, DC 20530
202-305-2513
Fax: 202-307-0345
Email: Grant.D.Johnson@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
05/31/2023	<u>1</u>	COMPLAINT against USA (DOD) (Filing fee \$402, Receipt number CFC100005882) (Copy Served Electronically on Department of Justice), filed by LARRY GOLDEN. Answer due by 8/4/2023. (Attachments: # <u>1</u> Civil Cover Sheet, # <u>2</u> Exhibit)(vds) Modified on 6/8/2023 to add receipt number (mjk). Modified on 6/14/2023 to edit response date (vds). (Entered: 06/05/2023)
06/05/2023	<u>2</u>	Notice of Random Assignment Pursuant to Rule 40.1(a) to Judge Matthew H. Solomson. (vds) (Entered: 06/05/2023)
06/05/2023	<u>3</u>	NOTICE of Non-ECF Case. (vds) (Entered: 06/05/2023)
06/05/2023	<u>4</u>	GENERAL ORDER No. 2022-01 dated 9/12/2022 continuing the suspension of paper filing requirements in pro se cases: Consistent with this court's General Orders issued on 3/18/2020, 11/13/2020, 12/23/2020, and 3/3/2021, it is ordered that judges, special masters, the Clerk of Court, and counsel of record for the United States may file electronically in pro se cases using the court's Case Management/Electronic Case Filing (CM/ECF) system. Pro se litigants shall, absent extraordinary circumstances, submit all case filings via e-mail to ProSe_case_filings@cfc.uscourts.gov. Pro se litigants may, if feasible, receive notification by e-mail of all electronic filings by filing an E-Notification Consent Form, attached to the General Order. (vds) Service on parties made. Docket nos. 2,3,4, sent first class mail on 6.5.23 ac7. (Entered: 06/05/2023)
06/12/2023	<u>5</u>	NOTICE of Appearance by Grant Drews Johnson for USA . (Johnson, Grant) (Entered: 06/12/2023)

06/14/2023	<u>6</u>	NOTICE of Directly Related Case(s) [13-307], filed by USA <i>and Motion to Transfer to Senior Judge Eric G. Bruggink</i> . (Attachments: # <u>1</u> Exhibit 1 (Sixth Amended Complaint in Case No. 13-307), # <u>2</u> Exhibit 2 (Complaint in Golden v. Google (N.D. Cal.)))(Johnson, Grant) (Entered: 06/14/2023)
06/15/2023	<u>7</u>	ORDER TRANSFERRING CASE to Judge Eric G. Bruggink. Signed by Judge Matthew H. Solomson. (cmb) Service on parties made. Plaintiff served via first class mail on 06.20.2023 (mjk) . Modified on 6/20/2023 (mjk). (Entered: 06/15/2023)
06/15/2023	<u>8</u>	NOTICE of Reassignment. Case reassigned to Senior Judge Eric G. Bruggink for all further proceedings. Judge Matthew H. Solomson no longer assigned to the case. (vds) Plaintiff served via first class mail on 06.20.2023 (mjk) . Modified on 6/20/2023 (mjk). (Entered: 06/16/2023)
06/20/2023	<u>9</u>	MOTION for Summary Judgment, filed by LARRY GOLDEN. Service: 6/20/2023. Response due by 7/18/2023 . (Attachments: # <u>1</u> Exhibit)(vds) (Entered: 06/20/2023)
07/14/2023	<u>10</u>	MOTION to Dismiss pursuant to Rule 12(b)(6) , filed by USA. Response due by 8/11/2023 . (Attachments: # <u>1</u> Exhibit 1, # <u>2</u> Exhibit 2, # <u>3</u> Exhibit 3, # <u>4</u> Exhibit 4, # <u>5</u> Exhibit 5)(Johnson, Grant) (Entered: 07/14/2023)
07/14/2023	<u>11</u>	MOTION to Stay Briefing on Plaintiff's Motion for Summary Judgment (Dkt. 9) , filed by USA. Response due by 7/28/2023 .(Johnson, Grant) (Entered: 07/14/2023)
07/19/2023	<u>12</u>	MOTION for Disqualification, filed by LARRY GOLDEN. Service: 7/19/2023. Response due by 8/2/2023 . (Attachments: # <u>1</u> Exhibit, # <u>2</u> Exhibit)(vds) (Entered: 07/25/2023)
07/24/2023	<u>13</u>	MOTION to Strike <u>10</u> MOTION to Dismiss pursuant to Rule 12(b)(6) , filed by LARRY GOLDEN. Service: 7/24/2023. Response due by 8/7/2023 .(vds) (Entered: 07/25/2023)
07/25/2023	<u>14</u>	RESPONSE to <u>11</u> MOTION to Stay Briefing on Plaintiff's Motion for Summary Judgment (Dkt. 9) , filed by LARRY GOLDEN. Reply due by 8/1/2023 . Service: 7/25/2023.(vds) (Entered: 07/27/2023)
07/31/2023	<u>15</u>	REPLY to Response to Motion re <u>11</u> MOTION to Stay Briefing on Plaintiff's Motion for Summary Judgment (Dkt. 9) , filed by USA. (Johnson, Grant) (Entered: 07/31/2023)
07/31/2023	<u>16</u>	RESPONSE to <u>12</u> MOTION for Disqualification , filed by USA. Reply due by 8/7/2023 . (Johnson, Grant) (Entered: 07/31/2023)
07/31/2023	<u>17</u>	REPLY to Response to Motion re <u>13</u> MOTION to Strike <u>10</u> MOTION to Dismiss pursuant to Rule 12(b)(6) , <u>10</u> MOTION to Dismiss pursuant to Rule 12(b)(6) , filed by USA. (Johnson, Grant) (Entered: 07/31/2023)
07/31/2023	<u>18</u>	ORDER granting <u>11</u> Motion to Stay briefing on Plaintiff's motion for summary judgment; denying <u>13</u> Motion to Strike <u>10</u> MOTION to Dismiss pursuant to Rule 12(b)(6) Signed by Senior Judge Eric G. Bruggink. (jpk1) Service on parties made. Plaintiff served via first class mail on 08.01.2023 . (ac7) (Entered: 07/31/2023)
08/04/2023	<u>19</u>	REPLY to Response to Motion re <u>12</u> MOTION for Disqualification, filed by LARRY GOLDEN. Service: 8/4/2023.(vds) (Entered: 08/08/2023)
08/09/2023	<u>20</u>	RESPONSE to <u>10</u> MOTION to Dismiss pursuant to Rule 12(b)(6) , filed by LARRY GOLDEN. Reply due by 8/23/2023 . Service: 8/9/2023.(vds) (Entered: 08/10/2023)
08/21/2023	<u>21</u>	REPLY to Response to Motion re <u>10</u> MOTION to Dismiss pursuant to Rule 12(b)(6) , filed by USA. (Attachments: # <u>1</u> Exhibit 1)(Johnson, Grant) (Entered: 08/21/2023)
08/30/2023	<u>22</u>	MOTION for Judicial Notice, filed by LARRY GOLDEN. Service: 8/30/2023. Response due by 9/13/2023 . (Attachments: # <u>1</u> Exhibit A, # <u>2</u> Exhibit B)(vds) (Entered: 08/31/2023)
08/31/2023	<u>23</u>	NOTICE OF SUPPLEMENTAL AUTHORITIES, filed by LARRY GOLDEN. (Attachments: # <u>1</u> Exhibit A, # <u>2</u> Exhibit B, # <u>3</u> Exhibit C) Service: 8/31/2023.(vds) (Entered: 09/01/2023)

09/11/2023	<u>24</u>	RESPONSE to <u>22</u> MOTION for Judicial Notice , filed by USA. Reply due by 9/18/2023. (Johnson, Grant) (Entered: 09/11/2023)
09/13/2023	<u>25</u>	REPLY to Response to Motion re <u>22</u> MOTION for Judicial Notice, filed by LARRY GOLDEN. Service: 9/13/2023.(vds) (Entered: 09/13/2023)
04/04/2024	<u>26</u>	NOTICE, filed by USA <i>Regarding Related Proceedings.</i> (Attachments: # <u>1</u> Exhibit 1 (April 3, 2024 Order in Golden v. Google (N.D. Cal.)), # <u>2</u> Exhibit 2 (Exhibit H to First Amended Complaint in Golden v. Google (N.D. Cal.)))(Johnson, Grant) (Entered: 04/04/2024)
04/10/2024	<u>27</u>	MOTION for Judicial Notice, filed by LARRY GOLDEN. Service: 4/9/2024. Response due by 4/24/2024. (Attachments: # <u>1</u> Exhibit 1)(vds) (Entered: 04/11/2024)
04/23/2024	<u>28</u>	REPORTED Order granting <u>10</u> MOTION to Dismiss pursuant to Rule 12(b)(6) filed by USA, The Clerk is directed to enter judgment. Signed by Senior Judge Eric G. Bruggink. (jpk1) Service on parties made. <i>Plaintiff served via certified mail on this day. Article no. 7018 0040 0001 1393 2942</i> Modified on 4/24/2024 (vds). (Main Document 28 replaced on 5/7/2024 to attach corrected PDF) (ypb). (Entered: 04/23/2024)
04/24/2024	<u>29</u>	JUDGMENT entered pursuant to Rule 58, that plaintiff's complaint is dismissed for failure to state a claim.(<i>Service on parties made. Plaintiff served via USPS</i>) (ar) (Entered: 04/24/2024)
04/30/2024	<u>30</u>	MOTION for Reconsideration, filed by LARRY GOLDEN. Service: 4/30/2024. (vds) (Entered: 05/03/2024)
07/17/2024	<u>32</u>	MOTION to Request Status Update on Motion for Reconsideration, filed by LARRY GOLDEN. Filed by Leave of the Judge Denied as Moot; See ECF <u>31</u> Service: 7/17/2024. (vds) Modified on 8/7/2024 (vds). (Entered: 08/07/2024)
07/30/2024	<u>31</u>	UNREPORTED ORDER denying <u>30</u> Motion for Reconsideration filed by LARRY GOLDEN and allowing filed motion for status update (received on 7/17/2024), and denying it as moot.. Signed by Senior Judge Eric G. Bruggink. (jpk1) Service on parties made. <i>Plaintiff served via First Class Mail on 08/02/2024</i> (km1). (Entered: 07/30/2024)
08/22/2024	<u>33</u>	NOTICE OF APPEAL, filed by LARRY GOLDEN. Filing fee \$ 605, receipt number CFC200000259. Copy to CAFC. (ac7) (Entered: 08/22/2024)
08/22/2024		Transmission of Notice of Appeal and Docket Sheet to US Court of Appeals for the Federal Circuit re <u>33</u> Notice of Appeal. (ac7) (Entered: 08/22/2024)
08/26/2024		CAFC Case Number 2024-2256 for <u>33</u> Notice of Appeal filed by LARRY GOLDEN. (ac7) (Entered: 08/26/2024)

23-811 C

Case No: _____

IN THE UNITED STATES COURT OF FEDERAL CLAIMS

Larry Golden

Plaintiff, Pro Se

740 Woodruff Rd., #1102

Greenville, South Carolina 29607

atpg-tech@charter.net

(864) 992-7104

LARRY GOLDEN,

Plaintiff,

V.

THE UNITED STATES DEFENSE
THREAT REDUCTION AGENCY

Defendant.

**Patent Infringement Pursuant to
28 U.S.C. Section 1498**

May 29, 2023

INFORMAL COMPLAINT

1. Under the Tucker Act, the United States Court of Federal Claims has jurisdiction to adjudicate a claim if the statute, regulation, or constitutional provision that is the basis for that claim “can fairly be interpreted as mandating compensation by the Federal Government for the damage sustained,” *United States v. Mitchell*, 463 U.S. 206, 217 (1983), and the plaintiff is “within the class of plaintiffs entitled to recover under the statute if the elements of [the] cause of action are established,” *Greenlee County, Arizona v. United States*, 487 F.3d 871, 876 (Fed. Cir.

SAppx1100

Received - USCFC
MAY 31 2023

2007). “There is no further jurisdictional requirement that plaintiff make [] additional nonfrivolous allegation[s] that [he] is entitled to relief under the relevant money-mandating source.” *Jan’s Helicopter Serv., Inc. v. Federal Aviation Agency*. 525 F.3d 1299, 1307 (Fed. Cir. 2008).”

2. This is a claim pursuant to 28 U.S.C. § 1498(a) for recovery of Plaintiff’s reasonable royalties for the unlicensed use, manufacture for, or by the United States, inventions described in and covered by United States Patent Numbers: 9,096,189; 9,589,439, and 10,163,287. **Exhibits A, B, & C**

JURISDICTION

3. The jurisdiction of this Court is based on the provisions of 28 U.S.C. § 1498(a).

4. 28 U.S.C. § 1498(a): Whenever an invention described in and covered by a patent of the United States is used or manufactured by or for the United States without license of the owner thereof or lawful right to use or manufacture the same, the owner’s remedy shall be by action against the United States in the United States Court of Federal Claims for the recovery of his reasonable and entire compensation for such use and manufacture.

THE PARTIES

5. Plaintiff Larry Golden is a citizen of South Carolina and has a principal place of business (ATPG Technology, LLC), and residence at 740 Woodruff Road, #1102, Greenville, S.C. 29607.

6. Defendant, the UNITED STATES DEFENSE THREAT REDUCTION AGENCY (DTRA). The DTRA is both a defense agency and a combat support agency within the U. S. Department of Defense (DoD) for countering weapons of mass destruction and supporting the nuclear enterprise. DTRA provides cross-cutting solutions to enable the DoD, the United States Government, and international partners to deter strategic attack against the United States and its allies; prevent, reduce, and counter WMD and emerging threats; and prevail against WMD-armed adversaries in crisis and conflict. The Solicitation for this initiative is attached as **Exhibit D: DTRA HDTRA-19-S-0005 BAA Call CBI-01**

STANDARD(S) FOR REVIEW

7. When the United States Court of Appeals for the Federal Circuit in Plaintiff's cases *Golden v. Apple Inc. et al* Case No. 22-1229 and *Golden v. Google* Case No. 22-1267, before filing an opinion on 09/08/2022, the three Circuit Judges of Dyk, Taranto, and Stoll used as their standard of review the following:

"Under the pleading standards set forth in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), a court must dismiss a complaint if it fails to allege "enough facts to state a claim to relief that is plausible on its face." *Twombly*, 550 U.S. at 570. This standard "requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Id.* at 555 (citation omitted). A plaintiff must allege facts that give rise to "more than a sheer possibility that a defendant has acted unlawfully." *Iqbal*, 556 U.S. at 678 (citation omitted). In the patent context, this court has explained that a plaintiff need not "plead facts establishing that each element of an asserted claim is met," *In re Bill of Lading Transmission and Processing Sys. Pat. Litig.*, 681 F.3d 1323, 1335 (Fed. Cir. 2012) (citing *McZeal v. Sprint Nextel Corp.*, 501 F.3d 1354, 1357 (Fed. Cir. 2007)), but must plead "'enough fact[s] to raise a reasonable expectation that discovery will reveal' that the defendant is liable for the misconduct alleged." *Id.* at 1341 (alteration in original) (quoting *Twombly*, 550 U.S. at 556). We review the district court's dismissal of the complaint *de novo*. *Anand v. Ocwen Loan Servicing, LLC*, 754 F.3d 195, 198 (4th Cir. 2014)."

8. Upon review, the three Circuit Judges of Dyk, Taranto, and Stoll considered all of the previous cases directly related to the Apple and Google cases [case nos. 22-1229 and 22-1267] that was currently before the Circuit Court; and, the recommendations, decisions, opinions, and judgements.

9. The Circuit Judges decided not to dismiss Plaintiff's cases based on the number of times Plaintiff was forced to file because of Court errors [changing the cause of action; improperly petitioning the PTAB; giving the Government another chance at dismissing Plaintiff's case; making a Section 1491(a) the same as a Section 1498(a); CFC adjudicating a 35 U.S.C. Section 271(a) which is outside the Court's jurisdiction; making a violation of antitrust laws the same as 35 U.S.C. Section 271(a); wrongfully dismissing as duplicative; wrongfully

dismissing because of page count, etc.] The *Golden v. Apple* case was dismissed *without prejudice* for the following reason:

“Mr. Golden does not argue that the docketed complaint contains factual allegations beyond those contained in his original complaint or that the allegations in the docketed complaint do anything beyond listing the alleged infringed-upon patent claims and the alleged infringing devices. This is plainly insufficient. We see no error in the district court *without prejudice* dismissal of the Apple case.”

10. In *Golden v. Google* CAFC Case No. 22-1267, the case was Vacated and Remanded back to the District Court for the following reason: **Exhibit E**

“In the Google case, the district court again concluded that Mr. Golden’s complaint was frivolous. Here, however, Mr. Golden’s complaint includes a detailed claim chart mapping features of an accused product, the Google Pixel 5 Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189. The district court discounted this claim chart because it “contains the exact same language as the claim charts previously rejected by the Federal Circuit [in the 2019 case], although Google Pixel 5 Smartphone appears in the far-left column instead of Apple.” Dist. Ct. Op. at 4. But to the extent that the chart includes the “exact same language” as previously rejected charts, it is simply the language of the independent claims being mapped to. The key column describing the infringing nature of the accused products is not the same as the complaint held frivolous in the 2019 case. It attempts—whether successfully or not—to map claim limitations to infringing product features, and it does so in a relatively straightforward manner. We conclude that the district court’s decision in the Google case is not correct with respect to at least the three claims mapped out in the claim chart. Mr. Golden has made efforts to identify exactly how the accused products meet the limitations of his claims in this chart. On remand, the district court should allow the complaint to be filed and request service of process [] ... We express no opinion as to the adequacy of the complaint or claim chart except that it is not facially frivolous.”

11. The Defendants in both cases asked the three Circuit Judges of Dyk, Taranto, and Stoll to affirm dismissal of Plaintiff’s cases because the cases are “frivolous” and that Plaintiff is a “serial filer”. The Circuit Judges reviewed the District Court case and decided against it.

12. What that means is, the Defendant (Government the United States) is collateral estoppel from re-litigating the issue of “frivolousness”; the number of times Plaintiff has file cases; and the cause of actions of those cases, because the issues were actually litigated and conclusively resolved by the three Circuit Judges of Dyk, Taranto, and Stoll in *Golden v. Google* CAFC Case No. 22-1267.

13. Issue preclusion, or collateral estoppel, precludes a party [Government] from relitigating an issue actually decided in a prior case and necessary to the judgment. In a collateral estoppel case, the issue at the heart of the claim has already been raised and litigated in *Golden v. Google* CAFC Case No. 22-1267.

14. According to law, any and all defense pleadings of “frivolousness” the Government presents in this case to prejudice Plaintiff, after the *OPINION* filed on 09/08/2022 in *Golden v. Google* Case No. 22-1267, should be disregarded and stricken because of “issue preclusion” and “collateral estoppel”.

NATURE OF THE CASE

15. Plaintiff included in this complaint a claim chart that is practically identical to the Google complaint and claim chart. Stare decisis is the legal doctrine Plaintiff is relying on because it obligates this Court to follow historical cases when making a ruling on a similar case.

16. Stare decisis ensures Plaintiff that cases with similar scenarios and facts are approached in the same way. Simply put, it binds this Court to follow the legal precedent set by the Federal Circuit in its previous decision in *Golden v. Google* CAFC Case No. 22-1267.

17. To demonstrate this is not an incidental occurrence Plaintiff provided this Court with a smartphone comparison chart of the Google Pixel 5; Apple iPhone 12; Samsung Galaxy S21; LG V60 ThinQ 5G; & Asus/Qualcomm Smartphone for Snapdragon Insiders. The results are the same, they all have virtually identical elements in their alleged infringing products.

18. Plaintiff has cured the deficiencies identified in *Golden v. US CFC* Case No. 13-307C. Plaintiff responded to the deficiencies only because this Court allowed the Government to present a defense whereby the sensors had to by “native” to the alleged infringing products. The Federal Circuit disagreed in *Golden v. Google* CAFC Case No. 22-1267 and determine the detection capability can also be CBRN plugins. Third party contractors cannot be held liable for

infringement if performing work for the Government, and with the Government's authorization and consent.

19. Plaintiff has reproduced a claim chart in this complaint that illustrates sensing mechanisms "native" to the smartphones manufactured by Google, Apple, Samsung, LG, and Qualcomm. The sensing mechanisms include the smartphone cameras, standard sensors, and ports.

20. To support Plaintiff's claim of products (communication devices) grouped together by common features of design similarities of at least that of a smartphone, a PC, etc. Plaintiff added to the smartphone group a Hewlett Packard PC to demonstrate infringement.

VIOLATION ALLEGED

The United States Department of Defense, "Defense Threat Reduction Agency (DTRA)" has Authorized and Consented to the Infringement of Plaintiff's Patents.

21. Upon information and belief, the United States Defense Threat Reduction Agency (DTRA), (the United States), beginning in year 2019, with the initiative DTRA HDTRA-19-S-0005 BAA Call CBI-01 has allegedly infringed claim 5 of Plaintiff's '287 patent, claim 23 of Plaintiff's '439 patent, and claim 1 of Plaintiff's '189 patent. Pursuant to the guidelines of 28 U.S.C. § 1498(a): "[w]henver an invention described in and covered by a patent of the United States is used or manufactured by or for the United States without license of the owner thereof or lawful right to use or manufacture the same, the owner's remedy shall be by action against the United States in the United States Court of Federal Claims for the recovery of his reasonable and entire compensation for such use and manufacture", Plaintiff believes the DTRA has "authorized or consented" to the infringement of Plaintiff's '287, '439, and '189 patents.

22. As a result of implied authorization or consent; the DTRA required the contractors of Draper, Microsoft, Intel, Hewlett Packard, Google, Apple, Samsung, LG, and Qualcomm to integrate "for the Government" its, hazard-awareness-and-response tools into the ATAK, iTAK, and WinTAK for chemical and biological agents and radiological and nuclear threats (CBRN) detection and reporting. Further, the contractors integrated, assembled, modified, or developed CBRN plugins for an end-user device such as Plaintiff's patented smartphones, PCs, and tablets.

AUTHORIZATION OR CONSENT

23. The Research & Development Directorate, Chemical and Biological (RD-CB) Department of the Defense Threat Reduction Agency (DTRA) issued on May 7, 2019, a Broad Agency Announcement (BAA) Call CBI-01 “Chemical and Biological Threats: Tactical Assault Kit (TAK) Plugins for Warning & Reporting and Decision Making” under BAA HDTRA1-19-S-0005.

24. Under the implied authorization or consent, Draper, Microsoft, Google, Apple, Samsung, LG, Qualcomm, Intel, and Hewlett Packard have “manufactured for the Government” products and devices that allegedly infringes claim 5 of Golden’s ‘287 patent, claim 23 of Golden’s ‘439 patent, and claim 1 of Golden’s ‘189 patent.

25. The government’s authorization of or consent to a contractor’s infringing activity may be express or implied, *TVI Energy Corp. v. Blane*, 806 F.2d 1057, 1060 (Fed. Cir. 1986); *Hughes Aircraft Co. v. United States*, 534 F.2d 889, 901 (Ct. Cl. 1976). To succeed on an implied authorization theory there must be some explicit government action, such as a contracting officer’s instruction, or evidence extrinsic to the contract language showing the government’s intention to assume liability, *Va. Panel*, 133 F.3d at 870; *Larson*, 26 Cl. Ct. at 370.

26. In *Larson v. United States*, the Claims Court recognized that implied authorization “may be found under the following conditions: (1) the government expressly contracted for work to meet certain specifications; (2) the specifications cannot be met without infringing on a patent; and (3) the government had some knowledge of the infringement.” *Larson*, 26 Cl. Ct. at 370 (citing *Bereslavsky v. Esso Standard Oil Co.*, 175 F.2d 148, 150 (4th Cir. 1949); *Carrier Corp. v. United States*, 534 F.2d 244, 247–50 (Ct. Cl. 1976); *Hughes*, 534 F.2d at 897–901).

27. The purpose behind permitting the government’s authorization or consent to be implied is tied to the government’s need to procure items without disruption, *TVI Energy*, 806 F.2d at 1060; *Robishaw Eng’g Inc. v. United States*, 891 F. Supp. 1134, 1145 (E.D. Va. 1995) (“[T]he policy purpose behind § 1498 is to insulate the government and its private contractors from ‘lawsuits disruptive of the procurement process.’” (quoting H.R. Rep. No. 872, 82d Cong., 1st Sess. 1420 (1951), as it appears in *Northrop Corp. v. McDonnell Douglas Corp.*, 705 F.2d 1030, 1041 (9th Cir. 1983))), and avoid the need for government agencies to perform an exhaustive patent search for products or services they wish to procure.

28. For example, in *TVI Energy*, the Federal Circuit found implied authorization or consent where the government required a contractor to demonstrate an allegedly infringing device as part of bidding requirements under a United States military solicitation for disposable thermal targets, 806 F.2d at 1060–61. Following the demonstration, one bidder/patent owner, TVI Energy, sued a competing bidder, Blane, for patent infringement. Blane asserted immunity under § 1498(a), despite having no express letter of consent or authorization from the government to infringe any patent. The Federal Circuit nevertheless found implied authorization, stating that “[t]o limit the scope of § 1498 only to instances where the Government requires by specification that a supplier infringe another’s patent would defeat the Congressional intent to allow the Government to procure whatever it wished regardless of possible patent infringement.”

29. Courts have often found a contractor, through the government’s implied authorization, to be immune from suit from the time it offers to supply or begin to manufacture products for the government, See, e.g., *Robishaw*, 891 F. Supp. at 1141 (citing *Trojan, Inc. v. Shat-R-Shield, Inc.*, 885 F.2d 854, 856–57 (Fed. Cir. 1989); *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 842 F.2d 1275, 1282–83 (Fed. Cir. 1988); *TVI Energy*, 806 F.2d at 1059–60; *Stelma, Inc. v. Bridge Elecs. Co.*, 287 F.2d 163, 164 (3d Cir. 1961)).

30. If these two elements—acting “for the government” with its “authorization or consent”—are met, then a contractor who infringes a patent in the course of its performance of work for the government, under any definition of infringement in § 271 of the Patent Act, is shielded from liability. In this respect, § 1498(a) serves as an affirmative defense available to government contractors in patent infringement actions in district court, *Advanced Software Design Corp. v. Fed. Reserve Bank of St. Louis*, 583 F.3d 1371, 1375 (Fed. Cir. 2009); *Toxgon Corp. v. BNFL, Inc.*, 312 F.3d 1379, 1381–82 (Fed. Cir. 2002).

31. Correlatively, where the government has assumed a contractor’s liability, a patent owner can seek judicial relief by filing suit against the government in the USCFC, *IRIS Corp. v. Japan Airlines Corp.*, 769 F.3d 1359, 1363 (Fed. Cir. 2014). However, various government agencies have internal processes to hear administrative claims for patent infringement. Christine Hlavka, Contractor Patent Bandits: Preventing the Government from Avoiding 28 U.S.C. § 1498 Liability for Its Contractors’ Unauthorized Use of Patented Material by Outsourcing One or More Steps of the Process Abroad, 37 Pub. Cont. L.J. 321, 324–25 (2008).

32. Therefore, for Draper, Microsoft, Google, Apple, Samsung, LG, Qualcomm, Intel, and Hewlett Packard “authorization or consent of the Government,” does not need to be expressly stated. *See TVI Energy Corp. v. Blane*, 806 F.2d 1057, 1060 (Fed. Cir. 1986) (“[a]uthorization or consent by the Government can be express [or] [i]n proper circumstances, Government authorization can be implied.”). Indeed, “authorization or consent . . . may be given in many ways other than by . . . direct form of communication--e.g., by contracting officer instructions, [or] by specifications . . . which impliedly sanction and necessitate infringement[.]” *Hughes Aircraft Co.*, 534 F.2d at 901.

33. In light of the allegations that the inventions disclosed in patents ‘287, ‘439 and ‘189 were designed to prevent terrorist activity, it is plausible that Draper, Microsoft, Google, Apple, Samsung, LG, Qualcomm, Intel, and Hewlett Packard manufactured infringing devices for the benefit of DTRA to promote national security’ see, e.g., *Hughes Aircraft Co.*, 534 F.2d at 898 (finding that the government’s participation in a satellite program was “for the Government,” because the program was vital to the military defense and security of the United States). Moreover, under section 1498(a), “Government authorization or consent” can be implied by circumstances. *See TVI Energy Corp.* 806 F.2d at 1060’

34. DTRA Government funding of research that led to the development and testing of the accused devices (e.g., CBNE Plugins; applications; chips) supports a reasonable inference that the Government impliedly sanctioned the infringing activity.

35. A review of the claim charts presented in this Complaint against the Defense Threat Reduction Agency (DTRA) identifies by name; by name and product number; or by name, model and product number, the devices that allegedly infringe Plaintiff’s patents.

ANDROID TEAM AWARENESS KIT (ATAK)

36. Android Team Awareness Kit (ATAK) is an Android smartphone geospatial infrastructure and military situation awareness app. It allows for precision targeting, surrounding land formation intelligence, situational awareness, navigation, and data sharing.

37. Android is a mobile operating system based on a modified version of the Linux kernel and other open-source software, designed primarily for touchscreen mobile devices such as smartphones and tablets. Android is developed by a consortium of developers known as

the Open Handset Alliance, though its most widely used version is primarily developed by Google. It was unveiled in November 2007, with the first commercial Android device, the HTC Dream, being launched in September 2008.

38. At its core, the operating system is known as Android Open-Source Project (AOSP) and is free and open-source software (FOSS) primarily licensed under the Apache License. Over 70 percent of smartphones based on Android Open-Source Project run Google's ecosystem (which is known simply as Android)

39. Android has been the best-selling OS worldwide on smartphones since 2011 and on tablets since 2013. As of May 2021, it had over three billion monthly active users, the largest installed base of any operating system

40. This Android app is a part of the larger TAK family of products. ATAK has a plugin architecture which allows developers to add functionality. This extensible plugin architecture that allows enhanced capabilities for specific mission sets (Direct Action, Combat Advising, Law Enforcement, Protection Operations, Border Security, Disaster Response, Off-grid Communications, Precision Mapping and Geotagging).

41. ATAK was initially created in 2010 by the Air Force Research Laboratory, and based on the NASA WorldWind Mobile codebase its development and deployment grew slowly, then rapidly since 2016. The Android Team Awareness Kit or TAK is currently used by thousands of Department of Homeland Security personnel, along with other members of the Homeland Security Enterprise including state and local public safety personnel. It is in various stages of transition across DHS components and is the emerging DHS-wide solution for tactical awareness.

42. In addition to the Android version, there is also a Microsoft Windows version (WinTAK), an Apple iOS version (iTAK), and finally a Virginia-based military tech firm's (LucyTAK). WinTAK is an application developed for the Microsoft Windows Operating System which uses maps to allow for precise targeting, intelligence on surrounding land formations, navigation, and generalized situational awareness. It was developed in conjunction with to provide similar functionality on a Windows platform.

43. In January 2015, AFRL began licensing ATAK through TechLink to U.S. companies, for commercial use to support state/local government uses as well as civilian uses. As of January 2020, one hundred companies have licensed ATAK for commercial uses. As of

March 31, 2020, the civilian version of ATAK, referred to as CivTAK has been approved for “Public Release” by Army Night Vision and is available for download on takmaps.com And subsequently named Android Team Awareness Kit (ATAK) - Civilian.

44. The Defense Threat Reduction Agency (DTRA) has leveraged TAK for enhanced CBRNE situational awareness with the goal of protecting military and civilian populations from intentional or incidental chemical or biological threats and Toxic Industrial Chemicals/Materials (TIC/TIM) hazards.

45. Under the Broad Agency Announcement from the Joint Science and Technology Office (JSTO) Digital Battlespace Management Division, DTRA funded the development of ATAK, WinTAK, and WebTAK compatible versions of existing decision support tools for chemical and biological warning and reporting, hazard prediction, and consequence assessment.

46. Through collaboration and innovation, the Defense Threat Reduction Agency has integrated its powerful, hazard-awareness-and-response tools into the Android Tactical Assault Kit (or the Android Team Awareness Kit, ATAK). ATAK is a digital application available to warfighters throughout the DoD. Built on the Android operating system, ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. Warfighters use ATAK to guide themselves to safety when confronted with a release of chemical and biological agents and radiological and nuclear threats (CBRN).

47. ATAK can connect to sensors on many platforms (e.g., satellites, drones, smartwatches) and has many plugins that warfighters can download. ATAK provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter’s vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.

48. Warfighters positively evaluated the CBRN plug-ins at the 2019 Chemical and Biological Operational Analysis (CBOA) event, where warfighters evaluated several technology prototypes for their utility in chemical and biological defense. Warfighters reported that the CBRN capabilities in ATAK are useful and easy to use with minimal training.

49. Overall, the U.S. armed forces and their interagency and coalition partners value ATAK and the common operating picture it provides. DTRA continues to develop CBRN-specific plug-in capabilities to support warfighters on the battlefield.

**SMARTPHONE COMPARISON BETWEEN THE GOOGLE PIXEL 5;
APPLE IPHONE 12; SAMSUNG GALAXY S21; LG V60 ThinQ 5G; & ASUS
/ QUALCOMM SMARTPHONE FOR SNAPDRAGON INSIDERS**

50. The Federal Circuit on 09/08/2022, in *Larry Golden v. Google LLC*; Case No. 22-1267 — “VACATED AND REMANDED” the relevant Case No: 22-1267 Document 15; back to the District Court “to be filed and request service of process”.


51. The Federal Circuit determined the complaint, “includes a detailed claim chart mapping features of an accused product, the Google Pixel 5 Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189” ... “in a relatively straightforward manner” ... and that the [Circuit] “express no opinion as to the adequacy of the complaint or claim chart except that it is not facially frivolous.” **Exhibit E**

Three-Judge Panel: “DISCUSSION. ‘Under the pleading standards set forth in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), a court must dismiss a complaint if it fails to allege “enough facts to state a claim to relief that is plausible on its face.” *Twombly*, 550 U.S. at 570 ... [T]his standard “requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” *Id.* at 555 (citation omitted). A plaintiff must allege facts that give rise to “more than a sheer possibility that a defendant has acted unlawfully.” *Iqbal*, 556 U.S. at 678 (citation omitted) ... this court has explained that a plaintiff ... must plead ““enough fact[s] to raise a reasonable expectation that discovery will reveal’ that the defendant is liable for the misconduct alleged.”

“Mr. Golden’s complaint includes a detailed claim chart mapping features of an accused product, the Google Pixel 5 Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189 ... It [claim chart] attempts [] to map claim limitations to infringing product features, and it does so in a relatively straightforward manner ... [W]e conclude that the district court’s decision in the Google case is not correct with respect to at least the three claims mapped out in the claim chart. Mr. Golden has made efforts to identify exactly how the accused products meet the limitations of his claims in this chart....”

Claim Chart for the Google Pixel 5 Smartphone (Federal Circuit)

The following Claim Chart is an illustration of literal infringement. At least one of the alleged infringing products of Google (i.e., Google Pixel smartphones 3, 3XL, 3a, 3aXL, 4a, 4a(5G), or 5) is representative of most all the above alleged infringing products of Google asserted in this complaint. At least one of the alleged infringing products of Google (Google Pixel 5) is illustrated to show how the Google Pixel 5 allegedly infringes on at least one of the asserted independent claims of each of the patents-in-suit ('287, '439, and '189 patents).

Google Pixel 5 Smartphone	Patent #: 10,163,287; Independent Claim 5	Patent #: 9,589,439; Independent Claim 23	Patent #: 9,096,189; Independent Claim 1
	A monitoring device, comprising:	A cell phone comprising:	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:
CPU: Octa-core (1 × 2.4 GHz Kryo 475 Prime & 1 × 2.2 GHz Kryo 475 Gold & 6 × 1.8 GHz Kryo 475 Silver) System-on-a-chip: Qualcomm Snapdragon 765G	at least one central processing unit (CPU);	a central processing unit (CPU) for executing and carrying out the instructions of a computer program;	at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;

<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures. Monitoring air temperatures.</p>	<p>at least one temperature sensor in communication with the at least one CPU for monitoring temperature;</p>	<p>X</p>	<p>X</p>
<p>Gravity sensor supported by the Android platform. Measures the force of gravity in m/s² that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).</p>	<p>at least one motion sensor in communication with the at least one CPU;</p>	<p>X</p>	<p>X</p>
<p>Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6-inch flexible OLED display at 432 ppi</p>	<p>at least one viewing screen for monitoring in communication with the at least one CPU;</p>	<p>X</p>	<p>X</p>
<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>at least one global positioning system (GPS) connection in communication with the at least one CPU;</p>	<p>at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;</p>

<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;</p>	<p>wherein at least one of... WiFi connection, internet connection, radio frequency (RF) connection, cellular connection... capable of signal communication with the transmitter or the receiver;</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group... of satellite, Bluetooth, WiFi...</p>
<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;</p>	<p>at least one of a... Bluetooth connection, WiFi connection, internet connection... cellular connection... short range radio frequency (RF) connection, or GPS connection;</p>	<p>X</p>
<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;</p>	<p>whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi-sensor detection systems, or to activate or deactivate the cell phone detection device;</p>	<p>X</p>

Pixel phones use USB-C with USB 2.0 power adapters and cables. To charge your phone with a USB-A power adapter, use a USB-C to USB-A cable.	at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;	X	X
<p>BIOMETRICS:</p> <p>Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;	wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and	wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use
<i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</i>	at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;	the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and	the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween...

<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p>one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;</p>	<p>at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>
<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU...</p>	<p>X</p>	<p>X</p>
<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</p>	<p>at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or... detect at least one of a chemical biological... agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.</p>	<p>a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p> <p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>

<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</p>	X	X	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems</p>
<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	X	<p>a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection... short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>

<i>Android Team Awareness Kit</i> , ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	X	whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.	X
--	---	---	---

I. Central Processing Units (i.e., CPUs, Processors, Chipsets, SoC)

1. Android Platform (i.e., Android Operating System (OS))

a. Application Specific for CBRNE Detection

i. Communication Protocol (i.e., Plug-ins, Bluetooth, Cellular, NFC)

The smartphone has come a long way since the first iPhone launched in 2007. While Apple's iOS is arguably the world's first smartphone operating system, Google's Android is by far the most popular. Android has evolved significantly since first being released on an HTC-made T-Mobile device in 2008.

It wasn't until 2005 that Google purchased Android, Inc., and while there wasn't much info about Android at the time, many took it as a signal that Google would use the platform to enter the phone business. Eventually, Google did enter the smartphone business — but not as a hardware manufacturer. Instead, it marketed Android to other manufacturers, first catching the eye of HTC, which used the platform for the first Android phone, the HTC Dream, in 2008.

List of Features Supported by Google Android Tactical Assault Kit, (ATAK) (or the Android Team Awareness Kit, (ATAK))

- ❖ **BIOMETRICS:** Biometric factors allow for secure authentication on the *Android platform*. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).
- ❖ **DISABLING LOCK MECHANISM:** *Google's Android operating system* features a lock mechanism to secure your phone, known as pattern lock. When setting the pattern, you must drag your finger along lines on the screen between different nodes. Afterward, to unlock the phone, you'll need to replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. If you can't log in, you'll have to employ some other methods to restore control of your phone.
- ❖ **CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR (CBRN) DETECTION:** Through collaboration and innovation, the Defense Threat Reduction Agency has integrated its powerful, hazard-awareness-and-response tools into the *Android Tactical Assault Kit (or the Android Team Awareness Kit, ATAK)*. ATAK is a digital application available to warfighters throughout the DoD. Built on the *Android operating system*, ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.
- ❖ **HEART RATE:** *Android Team Awareness Kit, ATAK* provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.
- ❖ **NEAR FIELD COMMUNICATION (NFC):** Pixel™, Phone by Google - Turn NFC on/off. *Near Field Communication (NFC)* allows the transfer of data between devices that are a few centimeters apart, typically back-to-back. NFC must be turned on for NFC-based apps (e.g., Tap to Pay) to function correctly. NFC is a set of short-range wireless technologies, typically requiring a distance of 4cm or less to initiate a connection. NFC allows you to share small payloads of data between an NFC tag and an Android-powered device, or between two Android-powered devices. Tags can range in complexity.
- ❖ **WARFIGHTERS:** The U.S. armed forces and their interagency and coalition partners value *Android Team Awareness Kit, ATAK* and the common operating picture it provides. DTRA continues to develop *CBRN-specific plug-in capabilities* to support warfighters on the battlefield.

The Alleged Infringing Smartphones Google, Apple, Samsung, LG, and Qualcomm that Support either the ATAК or the iTAK

Google Pixel 5 Smartphone	Apple iPhone 12 Smartphone	Samsung Galaxy S21 Smartphone	LG V60 ThinQ 5G	Asus / Qualcomm Smartphone for Snapdragon Insiders
				
<p>Chipset: Qualcomm Snapdragon 765G CPU: Octa-core (1 × 2.4 GHz Kryo 475 Prime & 1 × 2.2 GHz Kryo 475 Gold & 6 × 1.8 GHz Kryo 475 Silver) OS: Google Android 11, upgradable to Android 13. Modem: Snapdragon® X52 5G Modem-RF System.</p>	<p>Chipset: Apple A14 Bionic (5 nm). CPU: Hexa-core (2x3.1 GHz Firestorm + 4x1.8 GHz Icestorm). OS: iOS 14.1, upgradable to iOS 16.1 Modem: Qualcomm's Snapdragon X55 5G modem</p>	<p>Chipset: Qualcomm SM8350 Snapdragon 888 5G (5 nm). CPU: Octa-core (1x2.84 GHz Cortex-X1 & 3x2.42 GHz Cortex-A78 & 4x1.80 GHz Cortex-A55) - USA/China. OS: Google Android 11, upgradable to Android 13 Modem: Snapdragon® X60 5G Modem-RF System.</p>	<p>Chipset: Qualcomm SM8250 Snapdragon 865 5G (7 nm+). CPU: Octa-core (1x2.84 GHz Cortex-A77 & 3x2.42 GHz Cortex-A77 & 4x1.80 GHz Cortex-A55). OS: Google Android 10, upgradable to Android 13 Modem: Qualcomm's Snapdragon X55 5G modem</p>	<p>Chipset: Qualcomm SM8350 Snapdragon 888 5G (5 nm) CPU: Octa-core (1x2.84 GHz Cortex-X1 & 3x2.42 GHz Cortex-A78 & 4x1.80 GHz Cortex-A55). OS: Google Android 11. Modem: Snapdragon® X60 5G Modem-RF System.</p>
<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.</p>	<p>Temperature sensors located within; the sensors monitor the battery and processor's temperature. In extreme temperatures (hot or cold), these sensors shut down the device to prevent damage</p>	<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.</p>	<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.</p>	<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.</p>

Gravity sensor supported by the Android platform. Measures the force of gravity in m/s ² that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	Accelerometer (gravity sensor) supported by the iOS platform. Accelerometer/ Motion sensor: This sensor helps the screen automatically switch from landscape to portrait modes and back again based on whether you're holding the phone vertically or horizontally.	Gravity sensor supported by the Android platform. Measures the force of gravity in m/s ² that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	Gravity sensor supported by the Android platform. Measures the force of gravity in m/s ² that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	Gravity sensor supported by the Android platform. Measures the force of gravity in m/s ² that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).
Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6-inch flexible OLED display at 432 ppi	Adjusts the screen brightness for current light conditions using the built-in ambient light sensor. Screen: 6.1" Super Retina XDR (OLED). Lock the screen orientation so that it doesn't change when the iPhone is rotated.	Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.2 inches flexible OLED display at 421 ppi	Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.8 inches, 109.8 cm ² OLED display at 395 ppi density	Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.78 inches, 109.5 cm ² OLED display at 395 ppi density
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM) or Hybrid Dual SIM (Nano-SIM, dual stand-by)	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)

<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE, NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM)</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)</p>
<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE, NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM)</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)</p>
<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>Apple's iOS operating system features a lock mechanism to secure your phone. After multiple failed attempts to unlock the phone, the phone locks and is disabled (made unavailable).</p> <p>Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID / Touch ID or enter a passcode.</p>	<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>

<p>Pixel phones use USB-C with USB 2.0 power adapters and cables. To charge your phone with a USB-A power adapter, use a USB-C to USB-A cable.</p>	<p>USB-A to Lightning cable or the newer USB-C to Lightning cable with your iPhone. The MagSafe Battery Pack makes on-the-go, wireless charging easy and reliable—just attach it to your iPhone</p>	<p>Samsung USB-C Cable lets you charge your USB-C device as well as sync your data to your smartphone</p>	<p>UrbanX USB-C to USB 3.1 Adapter, USB-C Male to USB-A Female, Uses USB OTG Technology, Compatible with LG V60 ThinQ 5G</p>	<p>ASUS / Qualcomm Smartphone for Snapdragon Insiders Dual Port 32GB USB Type C Memory Stick; 32GB USB Type-C flash drive; Features USB Type-C connector and a traditional USB connector.</p>
<p>BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	<p>Apple's iOS operating system allows for Face ID authentication with the iPhone 12. The phone also features a lock mechanism to secure your phone. After multiple failed attempts to unlock the phone, the phone locks and is disabled (made unavailable).</p> <p>Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID, Touch ID, or enter a passcode.</p>	<p>BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	<p>BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	<p>BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>

<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</i></p>	<p><i>iOS Team Awareness Kit, iTAK (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</i></p>
<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>iOS Team Awareness Kit, iTAK (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>

<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual- band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual- band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE, NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD, NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano- SIM</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/ 6e, dual-band, Wi- Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)</p>
<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID / Touch ID, or enter a passcode.</p> <p><i>iOS Team Awareness Kit, iATAK (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>

<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</p>	<p>Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID-Touch ID or enter a passcode.</p> <p><i>iOS Team Awareness Kit</i>, iTAK (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies</p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</p>
<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>iOS Team Awareness Kit</i>, iTAK (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>

<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA’s contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>iOS Team Awareness Kit, iTAK (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA’s contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA’s contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA’s contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA’s contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>
--	--	--	--	--

Figure 1

Google’s “use” of Plaintiff’s Patented Central Processing Units (CPUs)

“[T]he Accused Products (i.e., Google, Apple, Samsung, LG, and Asus/Qualcomm smartphones), which are “computers” (i.e., cell phones, computer tablets, and laptops), include components of a memory, a display, and a **processor**” ... “[w]hen in use, the “Find My Device” pre-loaded onto the Accused Product uses a **processor**” ... “[t]he “Find My Device” feature displays [] information through a **processor** using data stored in the device’s memory” ... “[t]he LG Support Page lays out in a step-by-step process how to correctly remotely log in to the **processor** to access [] lock the device” ... See *Carolyn Hafeman v. LG Electronics Inc.*

In the above claim chart, the Google, Samsung, LG, and Asus/Qualcomm smartphones have Qualcomm Snapdragon Chipsets; have Octa-core CPUs (**processors**); have Google Android Operating Systems; have Qualcomm Snapdragon Modems; have Google “Find My Device” pre-installed See *Carolyn Hafeman v. LG Electronics Inc.*; have Google Android Team Awareness Kits; have Megapixel cameras for CBR sensing; have cameras for captioning nanopores; Biosensors for CBRNE detection; and, Plug-Ins for CBRN detection.

Figure 2 is a comparative chart of the “megapixel” smartphone cameras used for detecting Chem/Bio agents. For each different way used, it qualifies as an alternative to the ATAK or iTAK.

Google Pixel 5 Smartphone	Apple iPhone 12 Smartphone	Samsung Galaxy S21 Smartphone	LG V60 ThinQ 5G	Asus / Qualcomm Smartphone for Snapdragon Insiders
<p><i>Google Pixel 5: Dual - 12.2 MP (megapixel), OIS 16 MP (megapixel)</i></p> <p>Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A <i>megapixel</i> camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the <i>pixel</i> resolution phone camera. <i>Megapixel</i> resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. <i>Tiny sensors tucked into cell phones could map airborne toxins in real time.</i></p> <p>Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html</p>	<p><i>Apple iPhone 12: Dual - 12 MP (megapixel), OIS 12 MP (megapixel)</i></p> <p>Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A <i>megapixel</i> camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the <i>pixel</i> resolution phone camera. <i>Megapixel</i> resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. <i>Tiny sensors tucked into cell phones could map airborne toxins in real time.</i></p> <p>Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html</p>	<p><i>Samsung Galaxy S21: Triple - 12 MP (megapixel), OIS 64 MP (megapixel)</i></p> <p>Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A <i>megapixel</i> camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the <i>pixel</i> resolution phone camera. <i>Megapixel</i> resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. <i>Tiny sensors tucked into cell phones could map airborne toxins in real time.</i></p> <p>Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html</p>	<p><i>LG V60 ThinQ 5G: Dual - 64 MP (megapixel), OIS 13 MP (megapixel)</i></p> <p>Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A <i>megapixel</i> camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the <i>pixel</i> resolution phone camera. <i>Megapixel</i> resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. <i>Tiny sensors tucked into cell phones could map airborne toxins in real time.</i></p> <p>Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html</p>	<p><i>Asus / Qualcomm: Triple - 64 MP (megapixel) OIS; 8 MP, 12MP (mega)</i></p> <p>Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A <i>megapixel</i> camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the <i>pixel</i> resolution phone camera. <i>Megapixel</i> resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. <i>Tiny sensors tucked into cell phones could map airborne toxins in real time.</i></p> <p>Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html</p>

Figure 2

Figure 3 is a visual display of different ways the smartphone camera ^{1 2} can be used for detecting Chem/Bio agents. For each different way used, it qualifies as an alternative to the ATAК or iTAK.



Figure 3

1 The camera captures the image from the array of nanopores that uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the resolution phone camera. The resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time.* Source: [https:// www.understanding nano.com/cell-phone-sensors-toxins.html](https://www.understandingnano.com/cell-phone-sensors-toxins.html)

2 Hyperspectral imaging scans for light frequencies that humans can't see in order to identify the unique chemical signatures of different substances. They say their device, which can be mass produced, is compatible with all standard smartphone cameras. *These New Smartphone Cameras Could Tell You What an Object Is Made of* <https://www.sciencealert.com/new-smartphone-cameras-could-tell-you-what-an-object-is-made-of>

Figure 4 describes how at least nine (9) standard sensors for the Google, Apple, Samsung, LG, and Asus/Qualcomm smartphones can be used as “biosensors”. Each Biosensor qualifies as an alternative to ATA or iTA.

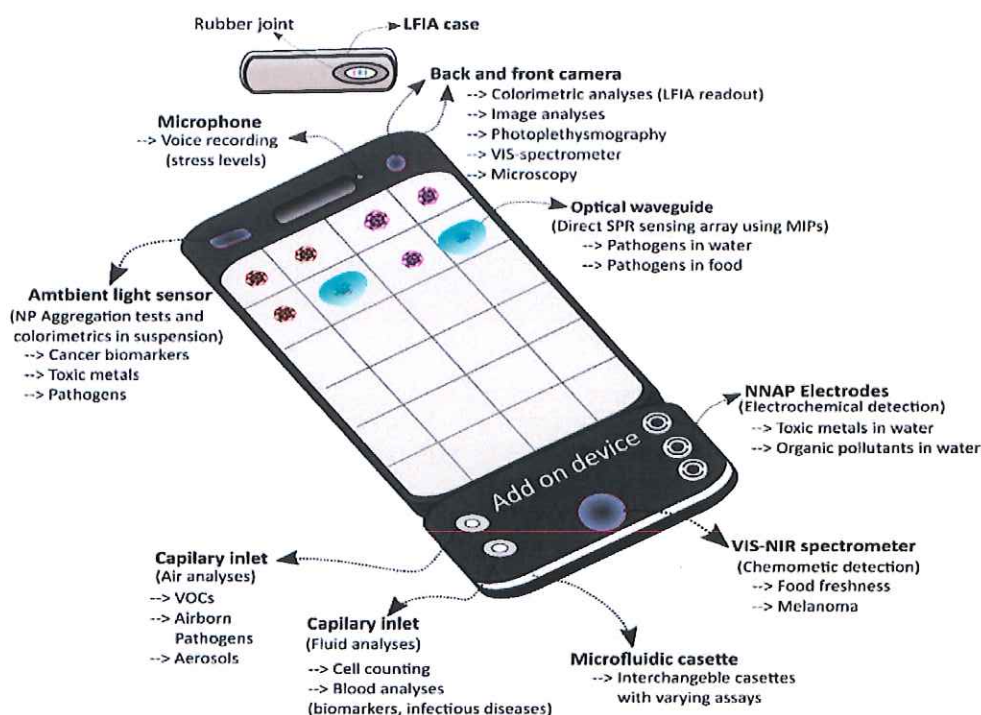


Figure 4

The Smartphones Biosensors:

1. Ambient light sensor: Cancer biomarkers; Toxic metals; Pathogens
2. Capillary inlet: (Air analysis). Airborne Pathogens; Aerosols
3. Capillary inlet: (Fluid analysis). Blood analysis; Biomarkers
4. Microfluidic cassette: Interchangeable cassettes with varying assays
5. VIS-NIR spectrometer: Food freshness; Melanoma
6. NNAP Electrodes: Toxic metals and Organic pollutants in water
7. Optical Waveguide: Pathogens in water and food
8. Back and front camera: Colorimetric analysis; Image analysis
9. Microphone: Voice recording stress levels

Figure 5 list some of the same standard sensors illustrated in Figure 4. The port on smartphones is used for the CBRN *plug-ins* included in ATAK or iTAK.

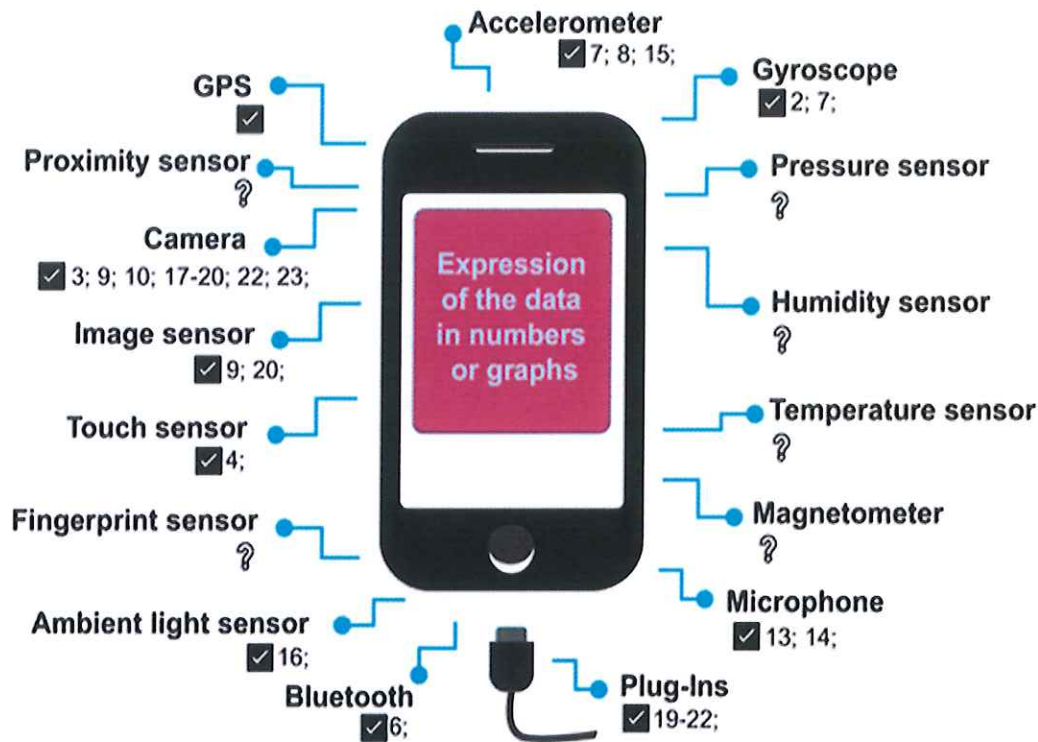


Figure 5

ATAK and iTAK are digital applications available to warfighters throughout the DoD. Built on the Android operating system and iOS operating systems, ATAK and iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK and iTAK now includes chemical, biological, radiological, and nuclear (CBRN) *plug-ins*.

Just having a plug-in is not all that's involved. There has to be an app specific software to sync the chemical, biological, radiological, and nuclear sensors to the smartphone plus the Google Android Operating System.

MICROSOFT WINDOWS (WINTAK)

52. In addition to the Android version (ATAK) CBRN plug-ins for smartphones, there is also a Microsoft Windows version (WinTAK). WinTAK is an application developed for the Microsoft Windows Operating System which uses maps to allow for precise targeting, intelligence on surrounding land formations, navigation, and generalized situational awareness. It was developed in conjunction with ATAK to provide similar functionality on a Windows platform.

53. The Defense Innovation Marketplace is your centralized source for Department of Defense (DoD) science and technology (S&T) planning, acquisition resources, funding and financial information. Under the Broad Agency Announcement from the Joint Science and Technology Office (JSTO) Digital Battlespace Management Division, DTRA funded the development of ATAK, WinTAK, and WebTAK compatible versions of existing decision support tools for chemical and biological warning and reporting, hazard prediction, and consequence assessment.

54. ATAK is an Android®-based GIS moving map application. WinTAK is Microsoft Windows®-based. ATAK was developed to provide SpyGlass-like C2, Situational Awareness and planning capabilities on smartphones and tablets. WinTAK was developed to provide a Windows-based application with a user interface similar to ATAK.

55. ATAK/WinTAK provides ground users and pilots a meaningful, geospatial site picture and inter-operates with other situational awareness tools including SpyGlass, RaptorX, FalconView, and other legacy systems. Both support most of the standardized image/map formats. Its standalone capabilities include moving map functions independent of cellular/Wi-Fi network. Additionally, these mobile applications allow maps to be loaded during mission pre-planning or execution phase. It utilizes internal and external GPS sources

56. ATAK/WinTAK variations are currently utilized by many branches of federal, state, and local governments and partner nations.

57. Draper, one of the nation's leading technology developers for national security, will build on its support for the warfighter under a new contract to operate and maintain the Tactical Assault Kit, or TAK, a widely used communications system for the military. The company recently received a sole-source contract with the Defense Threat Reduction Agency (DTRA) of the U.S. Department of Defense.

58. The \$415,000 contract calls for Draper to provide maintenance support, technical services, testing, evaluation and training for TAK. The TAK application supports the Nuclear Enterprise Contingency Operations Department's (NE-COs) various chemical, biological, radiological and nuclear (CBRN) detector systems.

59. Draper has developed software for every version of TAK since it was first developed by the Department of Defense. The software is available as ATAK for Android devices, WinTAK for Windows and WebTAK for the web. The company's long experience with the application and with warfighter systems overall were major reasons Draper will expand its role from research and development to operation and maintenance of the TAK platform, according to Brian Alligood, Draper's program manager for TAK. <https://www.draper.com/news-releases/draper-tapped-us-department-defense-provide-services-and-support-tactical-assault-kit>

60. Tactical Assault Kit (TAK) is a situational awareness solution designed for military and first responder personnel. On the original development team for ATAK for Android devices under the U.S. Air Force Research Laboratory, Draper contributed to initial design and core software. Draper also worked on WinTAK for Windows, and it developed WebTAK as a browser-based capability.

61. Draper designed a chemical, biological, radiological and nuclear (CBRN) Plugin to enable users to integrate CBRN sensors into TAK, collect CBRN sensor data, display it on a map and livestream it across the TAK network to other users. CBRN plugins for ATAK, WinTAK and WebTAK are operational in the field.

62. Below, is an illustrative claim chart of how the HP ZBook PC directly infringes claim 5 of Golden's '287 patent, and claim 1 of Golden's '189 patent.

63. To satisfy the limitation for CBRN that is internal the HP ZBook PC is Intel's Loihi Neuromorphic Chip to Learn and Recognize the Scents of 10 Hazardous Chemicals. Intel Labs' Nabil Imam holds a Loihi neuro-morphic chip in his Santa Clara, California, neuro-morphic computing lab. (Walden Kirsch/Intel Corp)

64. To satisfy the limitation for CBRN that is external the HP ZBook PC is WinTAK. WinTAK was developed to provide a Windows-based application. Draper designed a chemical, biological, radiological and nuclear (CBRN) Plugin to enable users to integrate CBRN sensors into WinTAK.

Exhibit 2

IN THE UNITED STATES COURT OF FEDERAL CLAIMS

LARRY GOLDEN,

Plaintiff,

V.

UNITED STATES,

Defendant.

1:13-cv-307-EGB

Senior Judge Eric G. Bruggink

August 22, 2021

PLAINTIFF’S CORRECTED PRELIMINARY INFRINGEMENT
CONTENTIONS—PATENT RULE 4(E)

Pursuant to this Court’s order, filed 07/29/2021 in this Case No. 13-307C; Dkt. No. 239, Plaintiff (“Larry Golden”) is filing his “Corrected Preliminary Infringement Contentions for Patent Rule 4(e)”.

The Corrected Preliminary Infringement Contentions illustrates that, “for each patent that claims priority to an earlier application, the priority date to which each asserted claim allegedly is entitled and whether the patentee [Plaintiff] is relying on the filing date or an earlier conception date as the priority date.” APPENDIX J: PATENT RULES OF THE UNITED STATES COURT OF FEDERAL CLAIMS; TITLE III. PATENT DISCLOSURES. Rule 4. Preliminary Disclosure of Infringement Contentions—(e). Plaintiff’s “Corrected Preliminary Infringement Contentions” are as follows:

- Thirty (30) alleged infringing products of Apple Inc. that, upon information and belief, Plaintiff is alleging infringes twenty-five (25) independent claims of Plaintiff’s ‘497, ‘752, ‘189, ‘439, & ‘287 patents.

- Twenty-seven (27) alleged infringing products of Samsung Electronics Inc. that, upon information and belief, Plaintiff is alleging infringes twenty-five (25) independent claims of Plaintiff's '497, '752, '189, '439, & '287 patents.
- Twenty-seven (27) alleged infringing products of LG Electronics Inc. that, upon information and belief, Plaintiff is alleging infringes twenty-five (25) independent claims of Plaintiff's '497, '752, '189, '439, & '287 patents.

PRIORITY AND CONCEPTION DATES

Each asserted independent claim of the '752, '189, '439, & '287 patents (i.e., 24 claims) are allegedly entitled to the filing date of the '497 patent.	Filing date of the '497 patent is <i>04/05/2006</i>
Each asserted independent claim of the '497, '752, '189, '439, & '287 patents (i.e., 25 claims) are allegedly entitled to the filing date of the Plaintiff's Disclosure Document filed with USPTO. Doc. No. 565732	Disclosure Document filed on <i>11/26/2004</i>
Each asserted independent claim of the '497, '752, '189, '439, & '287 patents (i.e., 25 claims) are allegedly entitled to the "conception of the technical rational"; inventions Plaintiff alleged are major components to the completion of Plaintiff's three economic stimulus packages submitted to the Government. The Affidavit submitted under 37 CFR §1.131 and §1.132 into record of the '752 patent (IFW) on 07/21/2010, establishes a priority date of Dec. 16, 2002 to overcome 102 and 103 objections. <i>A true copy of the document is attached</i>	Earlier conception filed with the Honorable Congressman Elijah E. Cummings: <i>12/16/2002</i>

All Twenty-Five Claims are Asserted Against the Following New and Improved Cell Phones (i.e., Smartphones) Manufactured and Used by Apple.

- Claim 1 of the '497 patent (Alleged infringing products are Apple iPhones 7, 8, SE, XS, 11, & 12)
- Claim 10 of the '752 patent (Alleged infringing products are Apple iPhones 7, 8, SE, XS, 11, & 12)

- Claims 1-9 of the ‘189 patent (Alleged infringing products are Apple iPhones 7, 8, SE, XS, 11, & 12)
- Claims 13-23 of the ‘439 patent (Alleged infringing products are Apple iPhones 7, 8, SE, XS, 11, & 12)
- Claims 4-6 of the ‘287 patent (Alleged infringing products are Apple iPhones 7, 8, SE, XS, 11, & 12)

All Twenty-Five Claims are Asserted Against the Following Watches, Chipsets, and CPUs Used by Apple.

- Representative Chart for Apple Watch Series 3, 4, 5, & 6
- Apple iPhone 7 Chipset: Apple A10 Fusion (16 nm).
- Apple iPhone 7 CPU: Quad-core 2.34 GHz (2x Hurricane + 2x Zephyr).
- Apple iPhone 8 Chipset: Apple A11 Bionic (10 nm).
- Apple iPhone 8 CPU: Hexa-core (2x Monsoon + 4x Mistral).
- Apple Watch Series 3 Chipset: Apple S3.
- Apple Watch Series 3 CPU: Dual-core
- Apple iPhone SE Chipset: Apple A9 (14 nm).
- Apple iPhone SE CPU: Dual-core 1.84 GHz Twister.
- Apple iPhone XS Chipset: Apple A12 Bionic (7 nm).
- Apple iPhone XS CPU: Hexa-core (2x2.5 GHz Vortex + 4x1.6 GHz Tempest).
- Apple Watch Series 4 Chipset: Apple S4.
- Apple Watch Series 4 CPU: Dual-core
- Apple iPhone 11 Chipset: Apple A13 Bionic (7 nm+).
- Apple iPhone 11 CPU: Hexa-core (2x2.65 GHz Lightning + 4x1.8 GHz Thunder).
- Apple iPhone 12 Chipset: Apple A14 Bionic (5 nm).
- Apple iPhone 12 CPU: Hexa-core (2x3.1 GHz Firestorm + 4x1.8 GHz Icestorm).
- Apple Watch Series 5 Chipset: Apple S5.
- Apple Watch Series 5 CPU: Dual-core.
- Apple Watch Series 6 Chipset: Apple S6.
- Apple Watch Series 6 CPU: Dual-core

All Twenty-Five Claims are Asserted Against the Following New and Improved Cell Phones (i.e., Smartphones) Manufactured and Used by Samsung.

- Claim 1 of the ‘497 patent (Alleged infringing products are Samsung Galaxy Note 8, Galaxy S8, S9, S10, S20, & S21)
- Claim 10 of the ‘752 patent (Alleged infringing products are Samsung Galaxy Note 8, Galaxy S8, S9, S10, S20, & S21)
- Claims 1-9 of the ‘189 patent (Alleged infringing products are Samsung Galaxy Note 8, Galaxy S8, S9, S10, S20, & S21)
- Claims 13-23 of the ‘439 patent (Alleged infringing products are Samsung Galaxy Note 8, Galaxy S8, S9, S10, S20, & S21)
- Claims 4-6 of the ‘287 patent (Alleged infringing products are Samsung Galaxy Note 8, Galaxy S8, S9, S10, S20, & S21)

All Twenty-Five Claims are Asserted Against the Following Watches, Chipsets, and CPUs Used by Samsung.

- Representative Chart for Samsung Gear S3 Classic Series, Galaxy Watch Active 2 Series, & Galaxy Watch 3 Series
- Samsung Galaxy Note 8 Series Chipset: Qualcomm MSM8998 Snapdragon 835 (10 nm) – USA/China
- Samsung Galaxy Note 8 Series CPU: Octa-core (4x2.35 GHz Kryo & 4x1.9 GHz Kryo) - USA & China
- Samsung Galaxy S8 Series Chipset: Qualcomm MSM8998 Snapdragon 835 (10 nm) – USA/China
- Samsung Galaxy S8 Series CPU: Octa-core (4x2.35 GHz Kryo & 4x1.9 GHz Kryo) - USA & China
- Samsung Gear S3 Classic Series Chipset: Exynos 7 Dual 7270 (14 nm)
- Samsung Gear S3 Classic Series CPU: Dual-core 1.0 GHz Cortex-A53
- Samsung Galaxy S9 Series Chipset: Qualcomm SDM845 Snapdragon 845 (10 nm) – USA/China
- Samsung Galaxy S9 Series CPU: Octa-core (4x2.8 GHz Kryo 385 Gold & 4x1.7 GHz Kryo 385 Silver)-USA/China

- Samsung Galaxy S10 Series Chipset: Qualcomm SM8150 Snapdragon 855 (7 nm) - USA/China
- Samsung Galaxy S10 Series CPU: Octa-core (1x2.84 GHz Kryo 485 & 3x2.42 GHz Kryo 485 & 4x1.78 GHz Kryo 485)-USA/China
- Samsung Galaxy Watch Active 2 Series Chipset: Exynos 9110 (10 nm)
- Samsung Galaxy Watch Active 2 Series CPU: Dual-core 1.15 GHz Cortex-A53
- Samsung Galaxy S20 Series chipset: Qualcomm SM8250 Snapdragon 865 5G (7 nm+) – USA
- Samsung Galaxy S20 Series CPU: Octa-core (1x2.84 GHz Kryo 585 & 3x2.42 GHz Kryo 585 & 4x1.8 GHz Kryo 585)-USA
- Samsung Galaxy S21 Series chipset: Qualcomm SM8350 Snapdragon 888 5G (5 nm)
- Samsung Galaxy S21 Series CPU: Octa-core (1x2.84 GHz Kryo 680 & 3x2.42 GHz Kryo 680 & 4x1.8 GHz Kryo 680)-USA
- Samsung Galaxy Watch 3 Series Chipset: Exynos 9110 (10 nm)
- Samsung Galaxy Watch 3 Series CPU: Dual-core 1.15 GHz Cortex-A53

All Twenty-Five Claims are Asserted Against the Following New and Improved Cell Phones (i.e., Smartphones) Manufactured and Used by LG.

- Claim 1 of the ‘497 patent (Alleged infringing products are LG V30, LG G6, LG G7, LG G8, LG V50, & LG V60)
- Claim 10 of the ‘752 patent (Alleged infringing products are LG V30, LG G6, LG G7, LG G8, LG V50, & LG V60)
- Claims 1-9 of the ‘189 patent (Alleged infringing products are LG V30, LG G6, LG G7, LG G8, LG V50, & LG V60)
- Claims 13-23 of the ‘439 patent (Alleged infringing products are LG V30, LG G6, LG G7, LG G8, LG V50, & LG V60)
- Claims 4-6 of the ‘287 patent (Alleged infringing products are LG V30, LG G6, LG G7, LG G8, LG V50, & LG V60)

All Twenty-Five Claims are Asserted Against the Following Watches, Chipsets, and CPUs Used by Samsung.

- Representative Chart for LG Watch Sport Series, LG Watch Style Series, & LG Watch W7 Series
- LG V30 Chipset: Qualcomm MSM8998 Snapdragon 835 (10 nm)
- LG V30 CPU: Octa-core (4x2.45 GHz Kryo & 4x1.9 GHz Kryo)
- LG G6 Chipset: Qualcomm MSM8996 Snapdragon 821 (14 nm)
- LG G6 CPU: Quad-core (2x2.35 GHz Kryo & 2x1.6 GHz Kryo)
- LG Watch Sport Chipset: Qualcomm MSM8909W Snapdragon Wear 2100
- LG Watch Sport CPU: Quad-core 1.1 GHz Cortex-A7
- LG G7 Chipset: Qualcomm SDM845 Snapdragon 845 (10 nm)
- LG G7 CPU: Octa-core (4x2.8 GHz Kryo 385 Gold & 4x1.7 GHz Kryo 385 Silver)
- LG G8 Chipset: Qualcomm SM8150 Snapdragon 855 (7 nm)
- LG G8 CPU: Octa-core (1x2.84 GHz Kryo 485 & 3x2.42 GHz Kryo 485 & 4x1.78 GHz Kryo 485)
- LG Watch Style Chipset: Qualcomm MSM8909W Snapdragon Wear 2100
- LG Watch Style CPU: Quad-core 1.1 GHz Cortex-A7
- LG V50 Chipset: Qualcomm SM8150 Snapdragon 855 (7 nm)
- LG V50 CPU: Octa-core (1x2.84 GHz Kryo 485 & 3x2.42 GHz Kryo 485 & 4x1.78 GHz Kryo 485)
- LG V60 Chipset: Qualcomm SM8250 Snapdragon 865 5G (7 nm+)
- LG V60 CPU: Octa-core (1x2.84 GHz Kryo 585 & 3x2.42 GHz Kryo 585 & 4x1.8 GHz Kryo 585)
- LG Watch W7 Chipset: Qualcomm MSM8909W Snapdragon Wear 2100
- LG Watch W7 CPU: Quad-core 1.3 GHz Cortex-A7

Plaintiff's is submitting his infringement contentions as a "Corrected Preliminary Infringement Contentions" that complies with Patent Rule 4. This is not an amendment. Plaintiff has always alleged the Defendants are infringing Plaintiff's central processing unit (CPUs). Plaintiff was ordered to identify the make and model of the CPUs in accordance to Patent Rule 4.

Respectfully submitted,

s/ Larry Golden

Larry Golden, Plaintiff, Pro Se

740 Woodruff Rd., #1102

Greenville, South Carolina 29607

atpg-tech@charter.net

864-288-5605

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 22nd day of August, 2021, a true and correct copy of the foregoing PLAINTIFF’S CORRECTED PRELIMINARY INFRINGEMENT CONTENTIONS—PATENT RULE 4(E) was served upon the following defendant via e-mail:

Grant D. Johnson
Trial Attorney
Commercial Litigation Branch
Civil Division
Department of Justice
Washington, DC 20530
Grant.D.Johnson@usdoj.gov
202-305-2513

Respectfully served by:

s/ Larry Golden
Larry Golden, Pro Se
740 Woodruff Rd., #1102
Greenville, South Carolina 29607
atpg-tech@charter.net
864-288-5605

Appeal No. 2024-2256

CERTIFICATE OF SERVICE

I hereby certify that on December 12, 2024 I electronically filed the foregoing Supplemental Appendix with the Clerk of the Court for the United States Court of Appeals for the Federal Circuit by using the appellate CM/ECF system, and served via e-mail on Plaintiff-Appellant Mr. Larry Golden at:

Larry Golden
atpg-tech@charter.net

/s/ Grant D. Johnson
GRANT D. JOHNSON